LAPIN AMK
Lapland University of Applied Sciences

HENKILÖTIETOJEN KÄSITTELY JA IDENTITEETTIVARKAUS

Katja Riva
Teija Valve

Opinnäytetyö
Yhteiskuntatieteiden, liiketalouden ja hallinnon ala
Liiketalouden koulutus
Tradenomi (AMK)

2015

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Yhteiskuntatieteiden, liiketalouden ja hallinnon ala

Liiketalouden koulutus

Tekijät Katja Riva ja Teija Valve 2015
Ohjaaja Merja Mattila
Työn nimi Henkilötietojen käsittely ja identiteettivarkaus
Sivumäärä 83

Henkilötietojen väärinkäyttö, jota kutsutaan myös identiteettivarkaudeksi, on jatkuvasti kasvava ongelma. Tämän opinnäytetyön tavoitteena on kuvata identiteettivarkauden eri muotoja, henkilörekistereitä koskevaa lainsäädäntöä sekä näitä seikkoja koskevia, tulevia lakimuutoksia. Työssä painopiste on henkilötietolain asettamissa määräyksissä, henkilörekistereissä sekä henkilötietojen väärinkäytösten kuvauksessa. Tutkimme myös, kuinka henkilö voi itse ennaltaehkäistä identiteettivarkaan uhriksi joutumista ja mitä toimenpiteitä rekisterinpitäjän tulee tehdä estääkseen rekisteröityjen henkilötietojen joutumisen vääriin käsiin.

Identiteettivarkaus on aiheena sikäli ajankohtainen, että se tekona tulee Suomessa rangaistavaksi 4.9.2015 voimaan tulevan rikoslain muutoksen yhteydessä. Lakimuutoksen taustalla on Euroopan unionin vuonna 2013 antama tietoverkkorikollisuuden torjuntaan tähtäävä direktiivi.

Tämä opinnäytetyö on laadullinen tutkimus, jonka lähteinä olemme käyttäneet pääasiassa aiheeseen liittyvää lainsäädäntöä sekä lainvalmisteluaineistoja. Tutkimustyössämme olemme halunneet käyttää laadukkaita ja ajantasaisia lähteitä. Aiheiden käsittelyssä olemme pyrkineet kattavaan mutta selkeään sisältöön.

Ihmisistä kerättävän tiedon määrä ja laatu on koko ajan kasvamassa ja toisaalta kerätyn tiedon hyödyntäminen tulee yrityksille koko ajan edullisemmaksi ja tekniikaltaan kehittyneemmäksi. Samalla mahdollisuudet käyttää näitä tietoja väärin lisääntyy. Lainsäädäntö ei ole pysynyt kehityksessä mukana ja näkisimmekin, että asialle pitäisi nopeasti tehdä jotain.

Avainsanat identiteetti, identiteettivarkaus, henkilötietolaki, henkilörekisteri

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

School of Business and Administration

Programme of Business Economics

Authors Katja Riva and Teija Valve 2015
Supervisor Merja Mattila
Subject of thesis Processing of personal information and identity theft
Number of pages 83

The misuse of personal information, also known as an identity theft, is a constantly growing problem. The purpose of this Bachelor's thesis is to look at the different forms of identity theft, legislations and regulations related to personal registers, as well as the legal changes needed. The focus of the thesis is on legislation and regulations regarding to the issues of the use of personal information, personal registers and descriptions of different forms for identity thefts. This thesis describes also how a person could prevent himself/herself from falling victim to identity theft and what the registrar should do to prevent misuse of registered personal information.

Identity theft will be officially recognized as a crime on 4 of September 2015 in Finland, due to the change to the legislation. This is to be consistent with the directive of EU, which was approved by the European parliament and council in 2013 in the purpose of preventing attacks on information systems.

This thesis is a qualitative study, and the prime sources of information have been laws and documents about law drafting, that are related to the subject. It is founded on high-quality and up to date information sources. This thesis aims to be an extensive and explicit work.

The quantity and quality of information that is gathered on people´s personal properties and doings is growing constantly and at the same time it is less expensive and more advanced technically to make the most of collected information and at the same time there are more and more opportunities to misuse this information. Legislation has not been able to keep up with this development and it is very important to rectify the situation as fast as possible.

Key words identity, identity theft, person register law, person register

Sisällys

1 JOHDANTO

1.1 Opinnäytetyön tavoite

Identiteettivarkaus, eli esiintyminen toisena henkilönä hänen henkilötietojaan käyttäen rikollisessa tai muuten asiattomassa tarkoituksessa, on internetin ja sosiaalisen median yleistymisen myötä kasvanut nopeasti. Tärkein työkalu identiteettivarkauden tekemiseen on henkilötunnus, ja teon onnistumisen apuna kaikki se tieto, mitä itse jaamme ja mitä meistä on tallennettu eri rekistereihin. Ihmisen luontaista taipumusta haluun uskoa hyvään ja luottaa toisiin ihmisiin käytetään häikäilemättä hyväksi. Identiteetin väärinkäyttö voi aiheuttaa uhrilleen monenlaista vahinkoa: taloudellisia menetyksiä, negatiivisia luottotietomerkintöjä, maineen menetystä ja mielipahaa. Asian selvittely voi olla pitkä ja raskas prosessi eikä välttämättä tule koskaan täysin selvitetyksi. Siksi jokaisen olisi tärkeää ymmärtää omien henkilökohtaisten tietojensa arvo ja käsitellä niitä sen mukaisella huolellisuudella.

Tämän opinnäytetyön tavoitteena on nostaa esille identiteettivarkaus ilmiönä ja kuvata sen eri muotoja sekä avata lukijalle henkilörekistereiden pitämistä koskevaa lainsäädäntöä. Kerromme myös tulevista sekä identiteettivarkautta että henkilörekistereitä koskevista lakimuutoksista. Käsittelemme myös hieman niitä erilaisia menetelmiä, joilla henkilötietojamme ja yksityisyytemme piiriin kuuluvia tietojamme kerätään ja hyödynnetään kaupallisesti. Työssä painopiste on henkilötietolain asettamissa määräyksissä, henkilörekistereissä sekä henkilötietojen väärinkäytösten kuvauksessa. Tutkimme myös, kuinka henkilö voi itse ennaltaehkäistä identiteettivarkaan uhriksi joutumista ja mitä toimenpiteitä rekisterinpitäjän tulee tehdä estääkseen rekisteröityjen henkilötietojen joutumisen vääriin käsiin. Vaikka identiteettivarkaudet ovat yleisempiä muualla maailmassa, rajasimme työmme koskemaan vain Suomea. Asia on noussut rikosten lisääntymisen johdosta yleiseksi puheenaiheeksi ja nyt myös ajankohtaiseksi tutkimusaiheeksi, koska identiteettivarkaus on tulossa rikoksena rangaistavaksi teoksi.

Henkilötietojen käsittelyä säätelevä lainsäädäntö on pääsääntöisesti tullut voimaan 1990-luvulla. Internetin yleisen kehityksen, sosiaalisen median suosion kasvun ja pilvipalveluiden yleistymisen aiheuttamaa muutosta henkilötietojen

käsittelyn määrässä tai menetelmissä ei tuolloin osattu vielä ennakoida. Henkilötietoja kerätään satoihin viranomaisrekistereihin ja tuhansiin kaupallisiin rekistereihin, tietoja ostetaan, myydään ja varastetaan. Tietoa, josta yksittäinen henkilö on mahdollista profiloinnin avulla yksilöidä, kerätään jatkuvasti. Lainsäädäntö on jäänyt jälkeen tekniikan ja menetelmien kehityksestä.

1.2 Tutkimusaineisto

Tämä opinnäytetyö on laadullinen tutkimus. Olemme käyttäneet lähdemateriaalina pääasiassa henkilötietolakia, rikoslakia sekä lainvalmisteluaineistoja, kuten hallituksen esityksiä sekä Euroopan komission esityksiä direktiiveiksi. Viranomaisohjeista olemme käyttäneet muun muassa valtiovarainministeriön julkaisemia VAHTI -ohjeita sekä tietosuojavaltuutetun toimiston julkaisemia materiaaleja. Lisäksi olemme perehtyneet henkilötietolakia ja yksityisyyden suojaa käsittelevään kirjallisuuteen. Tilastotietoa identiteettivarkauksien määrästä Suomessa ei ole saatavilla, koska sitä ei ole Suomessa kriminalisoitu, eikä sitä näin ollen tilastoida omana tekonaan rikostilastoihin. Visuaalisilla dokumenteilla, lähinnä televisiossa esitetyillä dokumentti- ja keskusteluohjelmilla, olemme saaneet kuvan identiteettivarkauden olemuksesta ja asian vakavuudesta. Kaikesta läpikäydystä aineistosta olemme pyrkineet järjestämään selkeän kokonaisuuden.

Tiedonhankinnassa ja aineistonvalinnassa pyrimme lähdekriittisyyteen ja ajantasaiseen tietoon. Aiheiden käsittelyssä pyrimme kattavaan mutta selkeään sisältöön.

2 HENKILÖ- JA IDENTITEETTITIEDOT

2.1 Henkilötiedot ja henkilöllisyys

Henkilöllisyys voidaan määritellä kokonaisuudeksi, joka muodostuu yksilöstä ja häneen liitetyistä väestötietojärjestelmään tallennetuista henkilötiedoista (Sisäasiainministeriö 2010, 17). Tällaisia perustietoja ovat muun muassa nimi, henkilötunnus, osoite, kotikunta, kansalaisuus, tiedot perhesuhteista sekä syntymästä ja kuolemasta. Henkilöllisyys muodostuu silloin, kun väestötietojärjestelmään luodaan tietue, jonka tiedot yhdistetään tavalla tai toisella koskemaan tiettyä fyysistä henkilöä. (Väestörekisterikeskus 2013.)

Henkilöllisyyden muodostavista tiedoista henkilötunnus on yksiselitteinen tunniste, jonka avulla henkilö voidaan erottaa kaikista muista henkilöistä ja jonka yhteyteen muut henkilötiedot voidaan viranomaistoiminnassa koota (Sisäasiainministeriö 2010, 17). Henkilötunnus on annettava henkilölle, kun hänen tietonsa ensimmäisen kerran tallennetaan väestötietojärjestelmään ja sen antamisesta vastaa Väestörekisterikeskus. Henkilötunnus on yksilöllinen ja sen muuttaminen on mahdollista ainoastaan laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista erikseen mainituissa tapauksissa. Tällainen erityistapaus on esimerkiksi tilanne, jossa väestötietojärjestelmään on tallennettu teknisesti virheellinen tieto. Henkilötunnus voidaan vaihtaa myös silloin, kun henkilötunnuksen muuttaminen on ehdottoman välttämätöntä henkilön terveyden tai turvallisuuden suojaamiseksi, tai kun muu kuin henkilötunnuksen haltija on aiheuttanut merkittävää haittaa tai taloudellista vahinkoa käyttämällä henkilötunnusta oikeudettomasti, eikä väärinkäytön jatkumista voida muutoin estää. (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009 2:11 § ja 12 §.) Maistraatin päätöksellä henkilötunnuksen voi vaihtaa myös silloin, jos henkilö on transseksuaalin sukupuolen vahvistamisesta annetun lain (563/2002) mukaisesti vahvistettu vastakkaiseen sukupuoleen kuuluvaksi (Väestötietojärjestelmä 2013.)

Henkilötunnuksen alkuosa on henkilön syntymäaika muodossa PPKKVV (päivä, kuukausi, vuosi). Seuraava merkki kertoo vuosisadan, jona hän syntyi. 1800 -luvulla syntyneillä merkki oli plus (+), 1900 -luvulla syntyneillä se on väliviiva (–) ja 2000 -luvulla syntyneillä se on kirjain A. Henkilötunnuksen loppuosan muodostaa kolmenumeroinen yksilönumero sekä tarkistusmerkki. Yksilönumero erottaa samana päivänä syntyneet henkilöt toisistaan. Yksilönumero on satunnainen, koneellisesti arvottu luku. Miehet saavat parittoman numeron, naiset parillisen. Tarkistusmerkki voi olla numero tai kirjain. Tarkistusnumero saadaan jakamalla syntymäajan ja yksilönumeron muodostama yhdeksännumeroinen luku 31:lla. Tulokseksi saadun jakojäännöksen perusteella katsotaan sitä vastaava tarkistusmerkki taulukosta (kuvio 1). Kun jakojäännös on desimaaliluku, kerrotaan desimaalit eli pilkun jälkeinen luku luvulla 31 ja saatu tulos pyöristetään lähimpään kokonaislukuun. Tätä kokonaislukua vastaava merkki tulee henkilön tarkistusnumeroksi. (Väestötietojärjestelmä 2013.)

Kuvio 1. Tarkistusmerkin laskeminen (Väestörekisterikeskus 2013)

Henkilötunnusta käytetään hyvin yleisesti henkilöllisyyden varmistamiseen, koska se on jokaisella erilainen. Ennen sirullisten pankkikorttien yleistymistä oli aivan normaalia kertoa henkilötunnuksensa loppuosa kaupan kassalle tämän sitä kysyessä, ja kenties muutamalle takana jonottavalle siinä samalla. Henkilöllisyyden todentamiseen henkilötunnus on kuitenkin erittäin huono väline, koska se on jossain määrin julkinen eikä sitä voi vaihtaa, kuin edellä kerrotuissa poikkeustapauksessa. (Järvinen 2010, 264.)

2.2 Identiteetti

Identiteetti (lat. identitas = samuus, täydellinen yhtenäisyys) tarkoittaa oman yksilöllisyyden kokemusta, henkilön käsitystä omasta itsestään. Se on siis vastaus kysymykseen kuka minä olen. Kyse on suhteellisen pysyvästä ja yhtenäisestä oman minän ja oman elämän kokemistavasta. Identiteetin tärkeimmät kehitysvaiheet ovat varhaislapsuus, murrosikä ja nuoruus. Identiteetti muodostuu samastumisen ja sosiaalisen oppimisen kautta ja sitä muokkaavat kokemukset ja vuorovaikutus muiden ihmisten kanssa. (Kalliopuska 2005, 77.) Identiteetti kuvaa henkilön elämän useaa eri osa-aluetta, jolloin käytetään esimerkiksi termejä kulttuuri-identiteetti, ammatillinen identiteetti, kansallinen identiteetti ja psykologinen identiteetti. Käytännössä sitä käytetään synonyymina henkilöllisyydelle. (Forss 2014, 83.)

Henkilötiedot ovat osa identiteettiä, mutta kokonaisuudessaan identiteetti käsittää kaikki ne tiedot, joilla yksilöt kyetään erottelemaan toisistaan. Ihminen ei kuitenkaan ole ainoa, jolla on identiteetti. Myös oikeushenkilöillä ja ryhmillä, joilla ei ole oikeudellista asemaa, on oma identiteettinsä. (Sisäasiainministeriö 2010, 17.) Oma identiteettinsä on myös esimerkiksi verkkoon kytketyllä tietokoneella, jolloin identiteetti rakentuu sen yksilöivistä tunnisteista, esimerkiksi IP-osoitteesta, domain-nimestä ja julkisesta avaimesta (Linden 2012,10).

Identiteetin peruselementtejä on kolmenlaisia: biometriset tunnisteet, annetut tai luodut tunnisteet sekä elämänkerralliset tunnisteet. Biometrisiä tunnisteita ovat sormenjäljet, DNA, ääni, iiris ja kasvonmuoto. Annettuja tai luotuja tunnisteita

ovat syntymäaika ja -paikka, nimi ja kansalaisuus. Elämänkerralliset tunnisteet tulevat osaksi ihmisen minuutta elämän varrella. Tällaisia tunnisteita ovat esimerkiksi koulutus, työhistoria ja avioliitto. (Sisäasiainministeriö 2010, 20–21.) Identiteetti on jokaiselle henkilölle osa hänen yksityisyyttään ja hänellä on siihen tiedollinen itsemääräämisoikeus, millä tarkoitetaan oikeutta tietää omien tietojen käsittelystä ja oikeutta vaikuttaa siihen. Tiedollisella omistusoikeudella tarkoitetaan oikeutta omaan nimeen, kuvaan ja hahmoon sekä oikeutta hallita niiden käyttämistä. (Sisäasiainministeriö 2010, 26.)

2.3 Digitaalinen identiteetti

Digitaalisen persoonan on kuvattu tarkoittavan mallia, joka perustuu yksilön julkisen persoonan tietoon, ja jota ylläpidetään tapahtumatietojen avulla. Sitä käytetään edustamaan yksilöä tietoverkoissa. (Heinonen 2001, 203.) Digitaalisen identiteetin tarkoitus on yksilöidä käyttäjä, erottaa hänet kaikista muista käyttäjistä. Digitaalinen identiteetti muodostetaan käyttövaltuustietojen, esimerkiksi käyttäjänimen ja salasanan taikka muiden luottamuksellisten tietojen, esimerkiksi henkilötunnuksen avulla (Limnéll–Majewski–Salminen 2014, 113). Tiedollisen itsemääräämisoikeuden, joka kuuluu jokaiselle omaan identiteettiinsä, tulisi koskea myös sähköistä identiteettitietoa, jolloin vain henkilöllä itsellään olisi oikeus päättää, pitääkö tiedon salassa vai julkistetaanko se (Sisäasiainministeriö 2010, 28).

Tunnistetiedot erottelevat käyttäjät toisistaan internetissä, mutta niiden avulla ei välttämättä voida tunnistaa käyttäjänä olevaa todellista henkilöä (Sisäasiainministeriö 2010, 17). Digitaalisesta identiteetistä puhuttaessa on hyvä huomata myös se, ettei sillä ole juurikaan tekemistä psykologisessa mielessä käytetyn, henkilön minäkuvasta kertovan identiteetti -termin kanssa. Digitaalinen identiteetti on puhtaasti vain tietojärjestelmään talletettu tietojoukko. (Linden 2012, 10.)

Viranomaisasioinnissa ja muissa virallisluonteisissa palveluissa, kuten esimerkiksi pankkipalveluissa, verkkoon kirjaudutaan aina vahvaa tunnistusmenetel-

mää käyttäen omana itsenämme. Sosiaalisessa mediassa voidaan kuitenkin toimia oman nimen käyttämisen lisäksi joko täysin anonyymina, nimimerkillä tai salanimellä eli pseudonyyminä. Tällöin verkkoidentiteetti voidaan muokata sellaiseksi, kuin halutaan. Verkkoidentiteetti voidaan luoda vaikka täysin vastakkaiseksi sille, mitä käyttäjä todellisessa elämässä on. Aktiivisesti verkkoa käyttävällä henkilöllä voi olla useita rinnakkaispersoonia ja saman henkilön verkkoidentiteetit voivat olla toisistaan hyvinkin poikkeavia. Monien kohdalla sähköpostiosoite on tekijä, joka yhdistää eri verkkoidentiteetit toisiinsa. (Aalto–Uusisaari 2009, 114–116.)

3 HENKILÖTIETOJEN KERÄÄMINEN

3.1 Henkilörekisterejä koskeva lainsäädäntö

Suomen perustuslaissa säädetään, että jokaisen yksityiselämä, kunnia ja kotirauha on suojattu. Lisäksi säädetään, että henkilötietojen suojasta säädetään erikseen lailla. (Perustuslaki 2:10 §.) Perustuslain velvoittamana on säädetty henkilötietolaki, jonka tarkoituksena suojata henkilötietojen asianmukaista käsittelyä sekä turvata itsemääräämisoikeutta ja vapautta (Pitkänen–Tiilikka–Warma 2013, 28). Henkilötietolain säädökset koskevat henkilötietojen automaattista eli tietoteknistä tai muutoin automatisoitua käsittelyä sekä henkilörekistereiden muodostamista. Lain määräyksiä sovelletaan silloin, kun rekisterinpitäjän toimipaikka on Suomessa tai muutoin Suomen oikeuskäytännön piirissä. Suomen oikeuskäytännön piiriin kuuluu rekisterinpitäjä, jolla ei ole toimipaikkaa Euroopan unionin jäsenvaltioiden alueella, mutta se käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita muuhunkin tarkoitukseen kuin vain tietojen siirtoon tämän alueen kautta. (Henkilötietolaki 523/1999 1:4 §). Tietojenkäsittelyn ulkoistuksen yleistyessä, tulee entistä vaikeammaksi hahmottaa se, minkä valtion lakeja henkilörekisterin ylläpitämisessä on noudatettava.

Henkilötiedolla tarkoitetaan kaikkea sellaista rekisterimerkintää, jolla kuvataan luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan ja jotka voidaan tunnistaa kyseistä henkilöä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa elävää koskeviksi tiedoiksi (Henkilötietolaki 523/1999 1:3 §). Tunnistettavissa olevan henkilötiedon yksiselitteinen määritteleminen on sangen vaikeaa. Tunnistaminen voi olla riippuvainen asiayhteydestä tai tilanteesta. Esimerkiksi väestötasolla yksittäisen henkilön tunnistaminen nimen perusteella ei onnistu, mikäli henkilön nimi on hyvin yleinen, mutta pienemmässä joukossa tunnistaminen on todennäköisempää. (Pitkänen ym. 2013, 44.) Matti Virtasen yksilöiminen pelkästään nimen perusteella koko Suomen väestöstä on mahdotonta, mutta työpaikalla taas yksilöiminen on helposti tehtävissä.

Henkilörekisterillä tarkoitetaan henkilötietoja sisältävää tietojoukkoa, joka koostuu käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä ja jota käsitellään osittain tai kokonaan tietotekniikan avulla tai joka on järjestetty kortistoksi, luetteloksi tai muuten sillä tavalla, että tiettyä henkilöä koskevat tiedot voidaan helposti löytää (Henkilötietolaki 523/1999 1:3 §). Henkilötietojen ei siis tarvitse olla tallennettuna tietokantaan tai muuhun tietotekniseen järjestelmään, jotta ne muodostavat henkilörekisterin. Riittää, että tiedot on koottu ja järjestetty siten, että yksittäisen henkilön tiedot voidaan löytää helposti eikä etsimisestä aiheudu kohtuuttomia kustannuksia. Tietosuojalautakunta on katsonut, että esimerkiksi taksin valvontakameran kuvista muodostuu henkilörekisteri, mikäli matkustajat ovat kuvista tunnistettavissa (Pitkänen ym. 2013, 54). Kuitenkaan yksityisen henkilön omaan käyttöön tarkoitetut rekisterit, kuten esimerkiksi puhelimen yhteystietoluettelo, eivät muodosta lain tarkoittamaa henkilörekisteriä.

Laki määrää suunnittelemaan henkilötietojen käsittelyn ja keräämisen ennen kuin henkilörekisteri perustetaan. Rekisterisuunnitelman laatimisessa voidaan hyödyntää rekisteritietojen elinkaarimallia (kuvio 2), jolloin tietojen käsittelyn vaiheet tulevat suunnitelmassa huomioiduksi. Rekisterisuunnitelmasta tulee käydä ilmi, millä tavalla kunkin tiedon käsittely on perusteltua rekisterinpitäjän toiminnan kannalta ja millaisten tehtävien hoitamiseksi tietoja käsitellään. Lisäksi on kerrottava, mitkä ovat tietojen lähteet eli kuinka tietoja säännönmukaisesti kerätään, mihin ja kenelle tietoja mahdollisesti luovutetaan sekä miten tarpeettomat tiedot poistetaan tai hävitetään. (Pitkänen ym. 2013,76-77.)

Kuvio 2. Henkilötietojen käsittelyn elinkaarimalli (Pitkänen ym. 2013, 77)

Henkilötietojen käsittelyn yleisistä edellytyksistä säädetään henkilötietolain 8 §:ssä ja henkilötietoja saa kerätä, käyttää, yhdistää, tallentaa tai luovuttaa vain silloin, kun on olemassa jokin kyseisessä pykälässä mainittu peruste. Lisäksi rekisterinpitäjän tulee huolehtia siitä, että muut henkilötietojen käsittelyä koske-

vat edellytykset, eli asiallisuusvaatimus ja tietojen käyttötarkoitussidonnaisuus, toteutuvat. (Pitkänen ym. 2013, 81–82.) Arkaluontoisten henkilötietojen ja henkilötunnusten käsittelystä säädetään vielä erikseen henkilötietolain 3. luvussa. Henkilötietoja saa lain mukaan käsitellä ainoastaan seuraavissa tapauksissa:

”1) Rekisteröidyn yksiselitteisesti antamalla suostumuksella”. Rekisteröidyn antamalla suostumuksella tarkoitetaan sitä, että henkilö on vapaaehtoisesti ja yksilöidysti ilmaissut hyväksyvänsä sen, että hänen henkilötietojaan käsitellään kyseisessä rekisterissä. Suostumuksen voi antaa suullisesti, kirjallisesti tai muulla tavoin, mutta suostumuksen osoitus ei kuitenkaan ole kyseessä silloin, kun henkilölle on varattu mahdollisuus kieltää tietojensa kerääminen, mutta hän ei ole sitä tehnyt. Suostumuksen pitää siis olla tietoisesti ja ilman sanktion uhkaa annettu tahdonilmaus. (Pitkänen ym. 2013, 61, 83.) Tämän säännöksen ongelmana on se, että henkilö ei aina välttämättä havaitse antavansa suostumusta tietojen rekisteröintiin. Esimerkiksi arvontaan osallistumisen yhteydessä hän voi huomaamattaan hyväksyä tietojensa keräämisen asiakasrekisteriin ja käyttämisen markkinointitarkoituksiin.

”2) Rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä”. Tällä säännöksellä tarkoitetaan tilannetta, jossa henkilö on sopimussuhteessa rekisterinpitäjään tai jonkun toisen tekemän sopimuksen vaikutuspiirissä. Toisen henkilön tekemän sopimuksen vaikutuspiiriin voi kuulua esimerkiksi asunnon vuokraustilanteessa, kun taloyhtiön isännöitsijälle on ilmoitettava kaikkien huoneistossa asuvien tiedot, vaikka vain yksi asukkaista on tehnyt vuokrasopimuksen. (Pitkänen ym. 2013, 84.)

”3) Jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi”. Silloin kun henkilötietojen käsittely on välttämätöntä rekisteröidyn hengen tai terveyden pelastamiseksi, se on sallittua. Kuitenkaan arkaluonteisia tietoja ei lähtökohtaisesti saa käsitellä edes edellä mainitussa tilanteessa ilman henkilön itse antamaa suostumusta. Tästä säännöksestä kuitenkin

voidaan poiketa, jos henkilö ei esimerkiksi tajuttomuuden vuoksi voi antaa suostumustaan ja hänen henkensä on vaarassa. (Pitkänen ym. 2013, 85.)

”4) Jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta”. Henkilötietojen käsittelystä säädetään varsinaisen henkilötietolain lisäksi useassa erityislaissa. Tällaisia erityislakeja ovat esimerkiksi laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009), laki yksityisyyden suojasta työelämässä (759/2004) ja Tietoyhteiskuntakaari (917/2014). Rekisterinpitäjällä voi siis olla erityislaissa säädetty velvollisuus kerätä henkilötietoja ja ylläpitää henkilörekisteriä. Rekisteröidyn tulee pystyä arvioimaan henkilötietojensa käsittelyn, keräämisen ja luovutuksen syyt ja laatu kyseessä olevasta säännöksestä. (Pitkänen ym. 2014, 86–87.)

”5) Jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (yhteysvaatimus)”. Asiallisella yhteydellä tarkoitetaan sitä, että rekisterinpitäjän ja rekisteröidyn välillä on jokin yhteys ja rekisteriä käytetään tämän yhteydenpidon hallinnoinnissa. Rekisterinpitäjän ja rekisteröidyn välille syntyy asiallinen yhteys esimerkiksi asiakassuhteen muodossa. Asialliseen yhteyteen perustuva henkilötietojen käsittely on rajattu koskemaan vain niitä tietoja, jotka ovat tarpeen kyseisen rekisterin pitäjän ja rekisteröidyn välisen suhteen hoitamisessa. Tarpeettomia tietoja ei saa kerätä ja henkilötiedot on poistettava rekisteristä, kun asiallista yhteyttä ei enää ole. (Pitkänen ym. 2014, 89–90.) Esimerkiksi työsuhteen päätyttyä työnantajan tulee poistaa työntekijää koskevat tiedot henkilöstörekisteristään siinä vaiheessa, kun niitä ei enää viranomaisille tehtäviä ilmoituksia varten tarvita.

”6) Jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä”. Tämä säännös mahdollistaa sen, että konsernissa tai muussa taloudellisessa yhteenliittymässä voidaan ylläpitää yhteisiä asiakas- tai henkilöstörekistereitä, vaikka rekisteriin kuuluva ei olisikaan kaikkien konsernin tai

yhteenliittymän jäsenen asiakas tai henkilöstön jäsen. Näin jokaisen konserniin kuuluvan yrityksen ei tarvitse ylläpitää omia rekistereitään vaan rekisterin pitäminen on keskitettyä toimintaa. (Pitkänen ym. 2014, 91.)

”7) Jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin verrattavia tehtäviä varten”. Henkilötietojen käsittely on sallittua myös silloin, kun se tapahtuu muun kuin varsinaisen rekisterinpitäjän toimesta, esimerkiksi ulkoistetun palvelun suorittamiseksi. Silloin, kun rekisterinpitäjä siirtää henkilötietojen käsittelyn ulkopuoliselle toimijalle, tulee asiasta tehdä ilmoitus tietosuojavaltuutetulle. (Pitkänen ym. 2014, 91.) Myös sen, jolle rekisterinpitäjä on siirtänyt henkilötietojen käsittelyn tehtäväksi, tulee tehdä toimintailmoitus tietosuojavaltuutetulle (Tietosuojavaltuutetun toimisto 2010d, 5).

”8) Jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi”. Henkilörekisterilain valmisteluvaiheessa on ajateltu, että laissa tarkoitettuja yleisesti saatavilla olevia tietoja ovat esimerkiksi kaupparekisteristä saatavat julkiset tiedot sekä yhteiskunnallisesti merkittävässä asemassa olevien henkilöiden tehtäviä kuvaavat tiedot, edellyttäen, että rekisteröinnillä on jokin merkitys jonkun henkilön tai henkilöryhmän etujen turvaamisessa. Esimerkiksi kansanedustajan työhön liittyvä julkinen tieto on tämän laikohdan tarkoittamaa tietoa. (Pitkänen ym. 2014, 92–94.)

”9) Jos tietosuojalautakunta on antanut käsittelyyn 43 §:n 1 momentissa tarkoitetun luvan.” Jos mikään pykälässä aiemmin mainituista edellytyksistä ei täyty, mutta henkilötietojen rekisteröinti ja käsittely on tarpeen laissa erikseen määrätyistä syistä, voi rekisterinpitäjä hakea luvan henkilötietojen käsittelyyn tietosuojalautakunnalta. Tällaisia erityisiä laissa määritettyjä syitä, joiden perusteella lupaa voi hakea, ovat:

- henkilötietojen rekisteröinnillä suojataan rekisteröidyn elintärkeää etua

- rekisteröinti on tarpeen yleistä etua koskevan tehtävän suorittamiseksi
- rekisteröinnin tarkoitus on mahdollistaa rekisterinpitäjälle tai tietojen luovutuksen saajalle kuuluvan julkisen vallan käyttämistä
- rekisteröinti on välttämätöntä rekisterinpitäjän tietojen luovutuksen saajan oikeutetun edun toteuttamiseksi, kuitenkaan vaarantamatta rekisteröityjen yksityisyyden suojaa ja oikeuksia (Pitkänen ym. 2014, 96).

Tietosuojalautakunnalle osoitettu lupahakemus on tehtävä kirjallisesti, mutta sille ei ole säädetty määrättyä muotoa. Siitä on kuitenkin käytävä ilmi rekisterin pitäjän tiedot, rekisterin tarkoitus, kenen ja mitä henkilötietoja käsitellään sekä perustelut ja hakijan yhteystiedot. (Pitkänen ym. 2014, 266.)

Laki asettaa rekisterille sekä tarpeellisuus- että virheettömyysvaatimuksen. Henkilötietojen tulee olla ennalta määritellyn tarkoituksen kannalta tarpeellisia, ja rekisterimerkintöjen käyttötarkoituksen määrittelyssä on ilmaistava se, millaisten tehtävien hoitamiseksi kyseisiä tietoja käsitellään (Pitkänen ym. 2013, 113). Rekisterinpitäjän on huolehdittava siitä, että virheellisiä, vanhentuneita tai epätäydellisiä tietoja ei käsitellä, vaan ne korjataan, täydennetään tai poistetaan rekisteristä asianmukaisesti (Henkilötietolaki 523/199 2:9 §).

Arkaluonteiseksi määriteltyjen henkilötietojen käsittely on lain mukaan pääsääntöisesti kielletty. Tällaisia tietoja ovat henkilön etnistä alkuperää tai rotua kuvaavat tiedot, yhteiskunnallista, poliittista tai uskonnollista vakaumusta kuvaavat tiedot, rikollista tekoa, rikosseuraamusta tai rangaistusta koskevat tiedot, terveydentilaan, hoitotoimenpiteisiin tai vammaisuuteen liittyvät tiedot, seksuaalista suuntautumista kuvaavat tiedot sekä sosiaalihuollon tarvetta tai palveluita koskevat tiedot. (Henkilötietolaki 523/1999 3:11 §.) Rekisterinpitäjä ei saa kiertää arkaluonteisten tietojen rekisteröintikieltoa rekisteröimällä sellaisia tietoja, joista arkaluonteinen tieto on selkeästi pääteltävissä joko suoraan tai eri tietoja yhdistelemällä (Pitkänen ym. 2013, 113). Poikkeuksista arkaluonteisten tietojen käsittelyssä säädetään henkilötietolain 523/1999 12 §:ssä.

Henkilötietolain 13 § määrää rekisterinpitäjää huolehtimaan siitä, että henkilötunnusta ei merkitä tarpeettomasti rekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin. (Henkilötietolaki 523/1999 13:4). Tämä momentti on tärkeä huomioida sekä elektronisissa asiakirjoissa, painetuissa materiaaleissa ja esimerkiksi sähköpostiviesteissä. Henkilöön liittyvää yksityiskohtaista tietoa on helppo saada paljon esimerkiksi sosiaalisen median kautta ja usein puuttuva palanen väärän identiteetin luomiseen on juuri henkilötunnus. Saadessaan henkilötunnuksen haltuunsa ja yhdistämällä sen kaikkeen muuhun keräämäänsä tietoon identiteettivarkaus on mahdollista toteuttaa. (Vanto 2011, 69.)

Rekisteriselosteen laatiminen on henkilötietolain 10 §:ssä rekisterinpitäjälle määrätty velvollisuus. Selosteesta tulee ilmetä rekisterinpitäjän ja tarvittaessa tämän yhteyshenkilön nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, se mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja EU:n tai Euroopan talousalueen ulkopuolelle sekä kuvaus rekisterin suojauksen periaatteista. (Henkilötietolaki 523/1999 2:10 §.) Tietosuojavaltuutetun toimisto on laatinut valmiin lomakkeen rekisteriselosteen laatimista varten. Rekisteriseloste on pidettävä jokaisen saatavilla. Tästä velvollisuudesta voidaan poiketa vain, jos se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi. (Henkilötietolaki 523/1999 2:10 §.) Rekisteriselosteen laajempi versio on tietosuojaseloste. Siinä on kaikkien rekisteriselosteessa mainittujen tietojen lisäksi kerrottu rekisteröidylle kuuluvat oikeudet; tarkastusoikeus, oikeus vaatia virheellisen tiedon korjaamista ja kielto-oikeus. (Pitkänen ym. 2013, 110.) Myös tietosuojaselosteen laatimista varten on valmis lomake tietosuojavaltuutetun internet sivuilla.

Jokaisella on oikeus saada rekisterinpitäjältä tieto siitä, mitä häntä koskevia tietoja henkilörekisteriin on tallennettu, jollei tarkastusoikeutta ole erikseen rajoitettu henkilötietolain 27 §:n perusteella. Tarkastusoikeutta on rajoitettu esimerkiksi tilanteissa joissa rekisteritietojen paljastuminen haittaisi rikostutkintaa tai olisi

uhka yleiselle turvallisuudelle tai henkilön itsensä turvallisuudelle. Myös tärkeän taloudellisen tai rahoitukseen liittyvän edun tai niihin liittyvän tarkastustehtävän vuoksi voidaan tarkastusoikeutta rajata. Poliisin, rikosseuraamusviraston, rajavartiolaitoksen ja puolustusministeriön rekistereiden osalta rekisteröity ei voi käyttää tarkastusoikeuttaan itse, vaan tarkastuksen voi tehdä vain tietosuojavaltuutettu. (Pitkänen ym. 2013, 203.) Rekisterinpitäjällä on myös velvollisuus ilmoittaa se, mitkä ovat rekisterin säännönmukaiset tietolähteet ja mihin tietoja luovutetaan ja käytetään. Tiedon voi pyytää kerran vuodessa maksutta. Useammin tapahtuvista pyynnöistä rekisterinpitäjällä on oikeus laskuttaa kohtuulliset ja tiedon antamisesta välittömästi aiheutuvat kustannukset. (Henkilötietolaki 523/1999 6:26 §.)

Henkilötietolain mukaan rekisterinpitäjällä on myös velvollisuus suojata henkilötiedot siten, että niihin ei pääse asiattomasti käsiksi eivätkä tiedot vahingossa tai laittomasti katoa, muutu tai niitä luovuteta eikä siirretä tai käsitellä muutoin laittomasti (Henkilötietolaki 523/1999 7:32 §). Rekisterinpitäjä on velvollinen korvaamaan vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle lainvastaisesta henkilötietojen käsittelystä. Korvausvelvollisuus ei edellytä laiminlyöntiä rekisterinpitäjältä, joten tässä noudatetaan ns. ankaran vastuun periaatetta, joka on tuottamuksesta riippumatonta. (Tietosuojavaltuutetun toimisto 2010b, 4.)

3.2 Viranomaisrekisterit

3.2.1 Väestötietojärjestelmä

Suomessa väestökirjanpitoa on pidetty jo 1500-luvulta lähtien. Kirjanpidon tarve on liittynyt sekä verotuksen että sotaväen saatavuuden tehostamiseen. Lisäksi kirkko on pitänyt omia rekistereitään syntyneistä, kastetuista, vihityistä ja kuolleista 1600-luvulta alkaen. Väestörekisteri on Suomen käytetyin perusrekisteri. Kaikista Suomen kansalaisista ja Suomessa vakituisesti asuvista ulkomaalaisista on tallennettu perustiedot väestörekisteriin. Rekisterin laissa säädetty tarkoitus on ylläpitää tietoja, jotka ovat tarpeen henkilön yksilöimisen, toimivaltaisuu-

den ja perhe- sekä henkilöoikeudellisen aseman selvittämistä varten. Henkilöön liittyviä perustietoja ovat muun muassa nimi, henkilötunnus, osoite, tiedot perhesuhteista, syntymä- ja kuolintieto sekä esimerkiksi tieto edunvalvonnasta tai uskonnollisen yhdyskunnan jäsenyydestä. (Väestörekisterikeskus 2015.) Tarkemmin henkilöstä väestötietojärjestelmään tallennettavista tiedoista on säädetty laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 13 §:ssä.

Väestötietojärjestelmässä näkyvät myös Maanmittauslaitoksen ylläpitämät yksilöintitiedot kaikista Suomessa sijaitsevista kiinteistöistä ja muista rekisteriyksiköistä. Tiedot päivittyvät väestötietojärjestelmään kerran viikossa. (Väestörekisterikeskus, 2013.) Yksilöintitietoja ovat kiinteistötunnus tai muu yksilöivä tunnistetieto, omistajan ja haltijan täydellinen nimi, yhteystiedot sekä henkilötunnus, syntymäaika tai yhteisöomistajan ollessa kyseessä y-tunnus (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009 2:14 §). Henkilö- ja kiinteistötietojen lisäksi väestötietojärjestelmään tallennetaan tiedot kaikista rakennuksista ja huoneistoista tunniste- ja omistajatietoineen sekä sijainnit koordinaatteineen. Tästä tietomassasta muodostuu osoitetietojärjestelmä. Lisäksi yhdistämällä kaikkia väestörekisterin henkilöistä, kiinteistöistä, huoneistoista ja rakennuksista koostettuja tietoja kiinteistö- ja rakennustunnuksiin ja rakennusten sijaintikoordinaatteihin, saadaan koostettua monipuolista paikkatietodataa muita yhteiskunnan rekistereitä ja paikkatietopalveluita varten. (Väestörekisterikeskus 2015.)

3.2.2 Kansaneläkelaitoksen rekisterit

Kansaneläkelaitoksen (Kela) yleistietokantoihin on tallennettu tiedot kaikista sellaisista henkilöistä, joilla on suomalainen henkilötunnus, henkilöistä joilla ei ole suomalaista henkilötunnusta, mutta jotka ovat hakeneet tai saavat jotain Kelan etuutta tai vaikuttavat haetun tai maksettavan etuuden määrään. Tällaisia henkilöitä ovat esimerkiksi asumistukea hakeneen kanssa samaan ruokakuntaan kuuluvat henkilöt. (Kansaneläkelaitos 2011, 2.) Yleistietojen tietokannoissa on yli 300 erilaista henkilöön liittyvää tietoa. Erilaisiin tietoryhmiin kuuluvat hen-

kilötiedot, asuinpaikkatiedot, perhesuhdetiedot, etuuksien viitetiedot sekä eläkehakemistotiedot. (Kansaneläkelaitos 2011, 3.)

Asiakasta koskevat henkilötiedot Kela saa Väestörekisterikeskukselta ja verotustiedot Verohallinnosta. Lainsäädännön perusteella työeläke- ja vakuutuslaitokset, työvoimaviranomaiset sekä sosiaali- ja terveysviranomaiset luovuttavat etuuksien myöntämiseen tai myönnettävään määrään vaikuttavia tietoja Kelalle. Suoranaisesti haettavaan etuuteen vaikuttavat muut tiedot saadaan asiakkaalta itseltään hänen jättämässään hakemuksessa ja tarvittaessa lisäselvityspyynnöllä. (Kansaneläkelaitos 2015.)

3.2.3 Verohallinnon rekisterit

Voidakseen toimittaa verotuksen, verohallinnon on kerättävä ja talletettava verotettavien henkilöiden henkilötietoja eri verolaeissa säädetyillä tavoilla. Verotuksen toimittamista varten ylläpidettävä rekisteri koostuu varsinaisesta tietojärjestelmästä ja siihen liittyvistä osarekistereistä. Esimerkkejä tällaisista osarekistereistä ovat muun muassa verokortti- ja ennakkoverorekisteri, osakehuoneistorekisteri ja perintö- ja lahjaverotusta varten ilmoitettujen vakuutusetuuksien rekisteri. Verotuksen tietojärjestelmään sisältyy myös julkisia rekistereitä. Tällaisia ovat esimerkiksi arvonlisäverovelvollisten rekisteri, ennakkoperintärekisteri ja verovelkarekisteri. (Verohallinto, 2015.)

Verohallinnon rekistereiden säännönmukaisia tietolähteitä ovat verovelvolliset itse sekä erilaiset tiedonantovelvolliset tahot. Henkilöasiakkaiden tiedonanto tapahtuu täydentämällä esitäytetty veroilmoitus ja antamalla muita selvityksiä tarpeen mukaan. Tiedonantovelvollisia tahoja ovat esimerkiksi työnantajat, eläkkeenmaksajat, rahoituslaitokset ja eri viranomaiset. Yrityksiltä saatava tieto liittyy esimerkiksi osinkoa jakavien yhtiöiden ilmoituksiin maksettujen osinkojen määrästä ja Suomen Asiakastieto Oy:n konkurssia, velkajärjestelyä tai liiketoimintakieltoa koskeviin tietoihin. (Verohallinto, 2015.)

3.2.4 Ajoneuvoliikennerekisteri

Ajoneuvoliikennerekisteriä ylläpitää Liikenteen turvallisuusvirasto Trafi. Rekisteriin merkitään muun muassa tiedot ajoneuvon omistajasta ja haltijasta, liikennevakuutuksen ottajasta sekä henkilöstä, jolla on ajo-oikeus (Laki ajoneuvoliikennerekisteristä 541/2003 2:1 § ja 3 §). Ajoneuvoliikennerekisterin ajo-oikeutta ja ajokorttia koskevia tietoja annetaan vain rajoitetusti, eli henkilö voi pyytää omista tiedoistaan ajokorttiotepyynnön, mutta ei ilman yksilöityä valtakirjaa toisen tiedoista (Liikenteen turvallisuusvirasto Trafi 2015).

Ajoneuvoja koskevat tiedot, kuten omistajatiedot osoitteineen ovat pääsääntöisesti kenen tahansa saatavilla ajoneuvoliikennerekisteristä. Mikäli henkilö ei halua, että hänen osoitetietonsa saa kysyttyä pelkästään ajoneuvon rekisteritunnuksen tietämällä, on hänen tehtävä erikseen osoitteenluovutuskielto ajoneuvoliikennerekisteriin. Kiellon voimassa ollessa ajoneuvon omistajan nimitieto on edelleen saatavissa. (Liikenteen turvallisuusvirasto Trafi 2015.)

3.3 Asiakasrekisterit ja internetin käyttäjäseuranta

3.3.1 Asiakasrekisterit ja kanta-asiakasjärjestelmät

Kaupallisille toimijoille asiakkaiden kulutustottumukset ja kiinnostuksen kohteet ovat rahanarvoista tietoa. Mitä paremmin myyjä tuntee asiakkaansa, sitä helpompaa on ennakoida tavarahankintoja, suunnitella myymälän tuotesijoittelua ja kohdentaa mainontaa tuote- ja asiakassegmenteittäin. Asiakkaan kannalta oikein kohdennettu mainonta on kätevää verrattuna siihen, että saisi jatkuvasti mainoksia tuotteista, joista ei ole lainkaan kiinnostunut. Tietoa ostoksista ja erilaisten palvelujen käytöstä sekä kiinnostuksen kohteista kerätään esimerkiksi markkinointitutkimuksilla, arvonnoilla ja kanta-asiakasjärjestelmillä. Kanta-asiakasjärjestelmissä asiakas saa etuja ja alennuksia vastineeksi siitä, että luovuttaa henkilötietonsa kauppiaalle ja sallii tämän kerätä ja hyödyntää tietoja ostoksista ja palveluiden käytöstä. (Järvinen 2010, 92–93, 96.) Esimerkiksi S-

ryhmän asiakasomistaja- ja asiakasrekisterin rekisteriselosteessa kerrotaan, että rekisterin tietosisältöön kuuluvat muun muassa seuraavat tiedot:

- asiakasomistajaetuihin oikeuttaviin ostoksiin käytetyn etukortin korttinumero tai jäsen-/asiointinumero
- ostopäivä
- kellonaika
- ostopaikka
- kortin käyttötapa
- tiedot ostoista kuitin loppusumma-, tuoteryhmä- ja/tai tuotetasolla (S-kanava 2014.)

Kerättävät tiedot mahdollistavat asiakkaan tarkan seurannan tuotetasolla ja esimerkiksi suosituimpien ostostentekoaikojen osalta. Kauppaketjujen ja niiden yhteistyökumppaneiden toimipaikat ja liiketoiminta-alueet kattavat miltei koko elämänkirjon, joten bonuskorttia ahkerasti käyttävän henkilön elintavat, harrastukset ja kiinnostuksen kohteet ovat kattavasti sekä kaupan että sen yhteistyökumppaneiden tiedossa ja siten hyödynnettävissä markkinointiin ja asiakkaan profilointiin (Järvinen 2010, 97–98). Kanta-asiakasjärjestelmiin pohjautuvassa tietojen keräämisessä ja analysoinnissa ei tarvitse edes yhdistellä useita eri rekistereitä yksilön tunnistamiseksi, koska kaikki tarvittava tieto on jo kaupan järjestelmissä. Lisäksi palveluntarjoajalla on mahdollisuus myydä keräämiään tietoja kolmannelle osapuolelle, joka usein mainitaan palvelusopimuksessa ja rekisteriselosteessa tarkemmin määrittelemättömänä yhteistyökumppanina.

3.3.2 Verkossa tapahtuva käyttäjäseuranta

Ihmiset hyödyntävät internetin ilmaisia palveluita mielellään ja rekisteröityessään antavat henkilötietojaan erilaisille palveluntarjoajille. Rekisteröitymisen yhteydessä palveluntarjoajat lähes poikkeuksetta tarjoavat mahdollisuutta tutustua yrityksen tietosuojakäytänteisiin ja lukea palvelun käytön ehdot, kuten henkilörekistereitä koskeva lainsäädäntö edellyttää, mutta kuinka moni oikeasti lukee sopimusehdot ja kuinka moni lukeneista todella ymmärtää, mihin sitoutuu

ja suostuu? On arvioitu, että yksittäisen ihmisen keskimäärin vuoden aikana käyttämien internetpalvelujen sopimustekstien lukemiseen menisi noin 30 työpäivää, jos ne todella luettaisiin huolellisesti (Heuer–Tranberg 2013, 31).

Erilaiset sosiaalisen median palvelut ovat tehneet henkilökohtaisten tietojen julkaisemisesta arkipäivää. Facebook, Twitter, Google+ ja muut vastaavat sosiaalisen median sovellukset keräävät päivittäin valtavan määrän tietoa ihmisten tekemisistä ja kiinnostuksen kohteista. Esimerkiksi yksin Facebookilla on yli miljardi rekisteröityä käyttäjää (Salo 2014, 46). Aika harvoin tilapäivitystä julkaistessaan tulee ajatelleeksi, että luovuttaa tiedon paitsi kaveripiirilleen, myös sille yhtiölle, jonka sosiaalisen median palvelua käyttää.

Google on yksi merkittävimpiä käyttäjätietoja keräävistä yrityksistä. Tunnetuin Googlen palveluista on tietysti hakupalvelu, josta on jo muodostunut verbi googlettaa synonyymiksi internetistä tapahtuvalle tiedonhaulle. Googlen liiketoiminta perustuu käyttäjätietojen ja kohdennettujen mainosten myymiseen, joten sen menestymisen kannalta on ensiarvoisen tärkeää kerätä mahdollisimman paljon tietoa palveluiden käyttäjistä (Järvinen 2010, 221). Hakupalveluiden lisäksi Googlen palveluvalikoimaan kuuluu muun muassa karttapalvelu Google maps ja mobiililaitteisiin saatava sijaintipalvelu Latitude, ilmainen sähköposti kalentereineen ja osoitekirjoineen, videopalvelu YouTube, toimisto-ohjelmisto Google-Docs, selain Chrome ja jopa käyttöjärjestelmä Chrome OS (Järvinen 2010, 224–225).

Googlen kohdennettu mainonta perustuu siihen, että yhtiö seuloo käyttäjiensä sähköposteja, nettihakuja ja sijaintitietoja ja etsii niistä tietoa käyttäjää kiinnostavista tuotteista ja palveluista. Google on ilmoittanut, että se on automatisoinut koko analyysiprosessin, eikä siis sen henkilökunta lue kenenkään sähköposteja, mutta toisaalta yhtiön johto on myös ilmoittanut, että se pyydettäessä luovuttaa käyttäjien tietoja viranomaisille. (Järvinen 2010, 223–224.)

Googlen lisäksi on olemassa muitakin käyttäjäseurantaan ja verkkomainontaan erikoistuneita yrityksiä. Lähes poikkeuksetta internetsivuihin on koodattu linkke-

jä erilaisiin mainospalveluihin, jotka seuraavat ja analysoivat käyttäjän toimia sivulla. Selain kertoo palvelimelle sen mistä maasta käyttäjät ovat, mistä he sivuille tulivat ja missä järjestyksessä sivuilla on liikuttu sekä paljon muuta. Selaimeen asennettavan ilmaisen laajennuksen Lightbeamin grafiikka (kuvio 3) havainnollistaa hyvin, millaisia määriä yhteyksiä kolmansiin osapuoliin muodostuu jo käynnistä viidellä yleisellä internetsivulla.

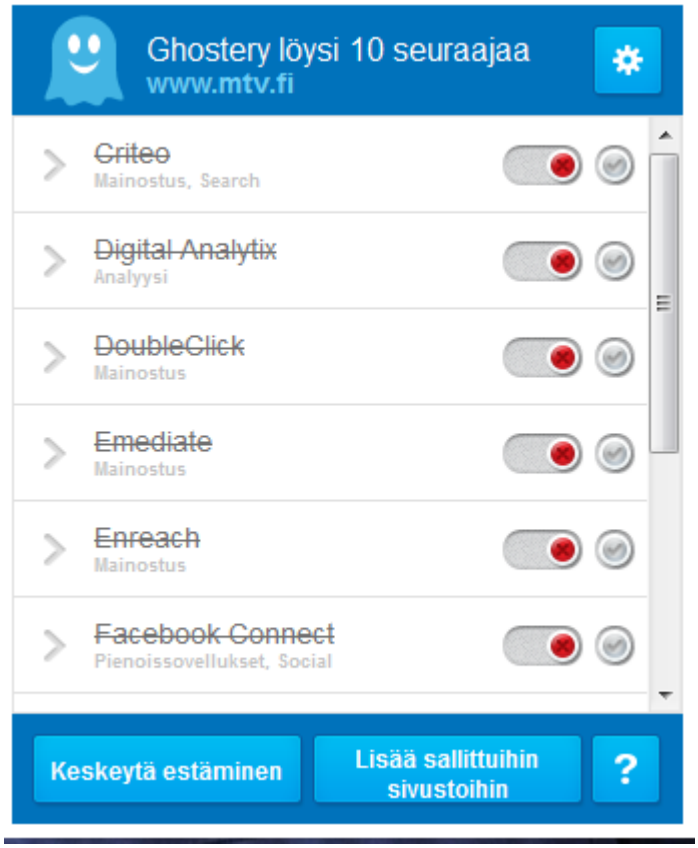
Kuvio 3. Yhteyksiä kolmannen osapuolen sivustoihin

Kokeilimme Lightbeam selainlaajennusta ja kävimme seuraavilla internetsivuilla:

- www.gmail.com
- www.mtv3.fi
- www.iltasanomat.fi
- www.iltalehti.fi
- www.facebook.com

Tuloksena oli yhteys 78 kolmannen osapuolen sivustoon. Eli yhteyksien määrä on moninkertainen vierailtuihin sivustoihin nähden.

Yhdysvalloissa on vuonna 2007 myönnetty patentti menetelmälle, joka analysoi käyttäjän sivustolla tekemien toimien perusteella tämän ominaisuuksia, kuten ikä, sukupuoli ja niin edelleen. Käyttäjäseurannalta voi halutessaan suojautua asentamalla selaimeen laajennuksen, joka estää käyttäjätietojen lähettämisen eteenpäin. Esimerkiksi testaamamme Ghostery ohjelma löysi ja esti sivustolta www.mtv3.fi kymmenen seuraajaa, kuten kuviosta 4 käy ilmi.



Kuvio 4. Lista estetyistä seuraajista

Tämän työn puitteissa meillä ei ole ollut mahdollisuutta tutustua näihin selainlaajennuksiin ja niiden käyttäjäehtoihin kuin aivan pintapuolisesti, joten emme sellaisenaan voi suositella juuri näitä käytettäväksi. Pidämme kuitenkin suositeltavana tutustua erilaisiin suojausvaihtoehtoihin ja harkita niiden käyttämistä yksityisyyden suojaamisessa.

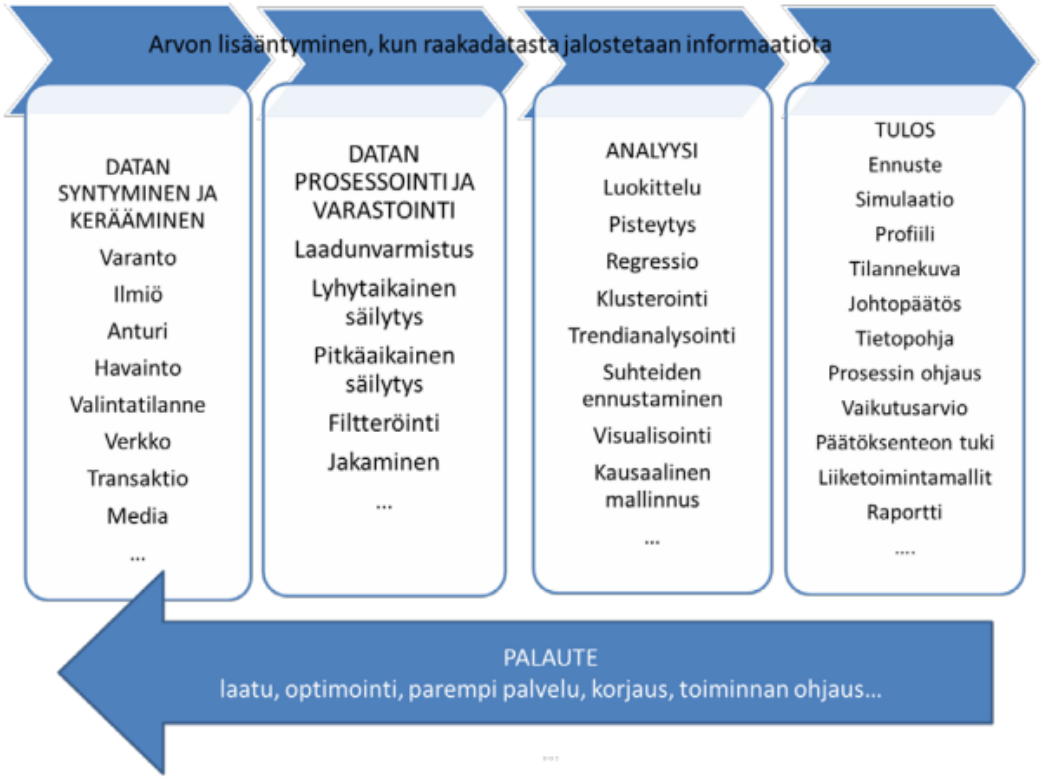
4 TIEDONKÄSITTELYN UUSIA SUUNTAUKSIA

4.1 Tiedon louhinta

Tiedon louhinnalla (data mining) ei ole tarkkaa määritelmää, mutta sillä viitataan tiedon erottamiseen suuresta datamäärästä (VTT Tietotekniikka 2000.) Datalla tarkoitetaan sitä suurta ja koko ajan nopeasti kasvavaa tietomäärää, joka toimii raaka-aineena sellaisen informaation etsimiseen, josta voidaan muodostaa käyttökelpoista tietoa. Teknologian kehitys on johtanut datamäärän vauhdikkaaseen kasvuun ja varsinkin internet tuottaa sitä kiihtyvällä nopeudella. Myös erilaiset mittausjärjestelmät, kuten sääasemat, navigointilaitteet, kauppojen videovalvontalaitteet sekä muut erilaiset sensorit ja reitittimet tuottavat dataa automaattisesti koko ajan. Kaikesta syntyvästä datasta, sen keräämisestä, säilyttämisestä ja analysoimisesta käytetään termiä Big data. Termillä viitataan paitsi datan suureen määrään (volume) myös sen vaihtelevuuteen (variety) ja vauhtiin (velocity). Digitaalisen datan määrää on käytännössä vaikea mitata, mutta luvuilla ilmaistaessa kyse on zettatavuista (ZB). Zettatavu on lukuna 10^{21}, eli luku, jossa on 21 nollaa. (Salo 2013, 11, 20–21). Big datan hyödyntämisellä haetaan etuja sekä yritysmaailmassa että julkisessa hallinnossa. Tavoiteltavat edut liittyvät toiminnan optimointiin ja siitä seuraaviin säästöihin, päätöksenteon tueksi saataviin tarkempien tietojen, tarkemman tilannekuvan saamiseen sekä tulevan ennustamiseen. (Liikenne- ja viestintäministeriö 2014, 8).

Tiedon louhinnassa on kyse niistä periaatteista ja tekniikoista, joita käytetään hyvin suurten tietomäärien tutkimisessa. Sitä käytetään, jotta löydettäisiin valtavaan datamäärään kätkeytyvää hyödyllistä tietoa, joka sitten jalostetaan käyttökelpoiseksi. Tiedon louhintaa käytetään esimerkiksi etsittäessä trendejä, malleja ja yhteyksiä. (VTT Tietotekniikka 2000.) Tiedon louhinnalla etsitään myös tiedon sisällä olevia lainalaisuuksia ja korrelaatioita, joiden avulla voidaan esimerkiksi helpottaa liiketoiminnan ennakoimista. Esimerkiksi kaupan kassajärjestelmästä voidaan tiedon louhinnan kautta selvittää, että tietyt kaksi tuotetta löytyvät useista ostoskoreista. Kauppa voi hyödyntää tiedon niin, että muuttaa tuotteiden sijaintia vastaamaan paremmin toistensa myyntiä tukevia tuotteita. Tie-

don louhinnalla kaupan alalla pyritään myös etsimään esimerkiksi syitä, miksi asiakkaat ovat siirtyneet kilpailijalle tai miten voidaan välttää tulevaisuudessa piileviä riskejä. Markkinoinnissa voidaan tiedonlouhintatekniikan avulla pyrkiä ennakoimaan kuluttajien käyttäytymistä esimerkiksi väestötietojen perusteella. Tiedonlouhinnassa käytetään tilastollisia, matemaattisia ja tietojenkäsittelyllisiä puoliautomaattisia analysointimenetelmiä. (Hovi–Hervonen–Koistinen 2009, 99.) Kuviossa 5 havainnollistetaan sitä, millä tavoin informaation jalostaminen lisää kerätyn tiedon arvoa.



Kuvio 5. Datan hyödyntämisen arvoketju. (Liikenne- ja viestintäministeriö, 2014, 9)

Kaikki se tieto, mitä meistä kerätään, päätyy tiedon louhinnan prosessiin. Sähköisten palveluiden käyttö eri päätelaitteilla kerää valtavasti dataa. Tietoa kerätään paitsi sillä, mitä palvelussa tehdään myös sillä, mitä jättää tekemättä. Pelkästään käymällä yrityksen verkkosivuilla, käyttäjä jättää jälkeensä runsaasti tietoa itsestään ja kiinnostuksen kohteistaan. Tietoa esimerkiksi meistä kuluttajina kalastellaan monin tavoin. Markkinointitutkimukset, joissa on mahdollisuus

voittaa vaikkapa tavarapalkinto, on yksi tapa saada kuluttaja luovuttamaan tietoja. Tiedonhankintaa tehdään myös epäsuoran palkitsemisen kautta antamalla tietoa vastaan palautetta tai palveluita. Esimerkiksi Googlen hakukone tallettaa tietoja käyttäjän kiinnostuksen kohteista ja antaa vastikkeeksi usein pitkänkin listan hakutuloksia. Sosiaalisen median palvelut, kuten Facebook, Google+ ja Twitter, ovat Big Datan digitaalisten lähteiden tunnetuimpia esimerkkejä. Palveluun rekisteröityessään käyttäjä luovuttaa tietojaan ja saa korvaukseksi haluamansa palvelun. Käyttäjien luovuttamien tietojen perusteella palvelua voidaan kehittää, mutta samalla voidaan myös harjoittaa liiketoimintaa. Esimerkiksi Facebook myy mainostajille kuluttajasegmenttejä, joiden avulla mainostajat voivat tavoittaa vaikkapa tietyn ikäiset ja tiettyä sukupuolta olevat ihmiset tietyllä alueella. (Salo 2013, 41–42).

Big Datalla ja tiedonlouhinnalla tuotetaan kuluttajille hyötyjä. Niiden avulla voidaan tuottaa yhä henkilökohtaisempaa palvelua. Palvelut ja tuotteet voidaan tarkentaa tehokkaammin ja edullisemmin vastaamaan kunkin käyttäjän tarpeita. Varjopuolena voidaan nähdä se, että tietojen luovuttamisen välttäminen on nykyaikana vaikeaa. Vaikka jättäytyisikin kauppojen kanta-asiakasjärjestelmien ulkopuolelle eikä asioisi verkkokaupoissa, kaiken teknologian välttäminen käy yhä vaikeammaksi. Uhkia liittyy myös tietosuojan varmistamiseen. Pilvipalveluiden yhteydessä puhutaan hunajapurkki-ilmiöstä: mitä suurempi on kohteessa oleva datamäärä, sitä houkuttelevampi kohde se on tietomurroille. Kaikkea tietoa voidaan käyttää väärin ja lainsäädäntö on aina jäljessä teknisestä kehityksestä. (Salo 2013, 41, 44–45).

4.2 Profilointi

Eri tietokannoista saatavia tietoja yhdistelemällä ja valittuja kriteerejä käyttämällä voidaan laajasta ihmisjoukosta luoda profiileja (Heinonen 2001, 170). Profilointeja varten voidaan kerätä dataa tunnistamalla päätelaitteita ja keräämällä tietoa niillä suoritettavista toimista. Asiakkaan ei siis tarvitse olla rekisteröitynyt palveluun eikä edes nähdä kyseistä palvelua, kun hänen toimistaan syntyy käyttäjäprofiilin tunnistamisen mahdollistava kuva. Riittävän pitkään jatkuneen pal-

velun käytön jälkeen kuva on niin yksityiskohtainen, että yksittäinen käyttäjä on hyvin pienin lisätiedoin yhdistettävissä oikeaan henkilöön reaalimaailmassa. Yksittäisen verkkopalvelun käyttäjän on mahdotonta tietää, ketkä kaikki keräävät hänen tietojaan ja profiloivat häntä. (Salo 2014, 54.) Profilointia käytetään hyväksi paitsi tietovalvonnassa myös kaupallisessa tarkoituksessa. Molemmissa tarkoituksissa profilointi voidaan ilmaista seuraavasti: *”Profilointi on tekniikkaa, jossa tiettyyn kategoriaan kuuluvan henkilön piirteet on johdettu menneestä kokemuksesta, ja siinä etsitään tietoja yksilöistä, jotka sopivat mahdollisimman tarkoin näihin piirteisiin”.* (Heinonen 2001, 170.)

Suomen lainsäädännössä profilointia ei ole määritelty lainkaan. Euroopan neuvosto on vuonna 2010 antanut suosituksen, että henkilötietojen keräämiseen ja käsittelyyn liittyvät suosituksessa luetellut periaatteet otetaan huomioon jäsenmaiden lainsäädännössä ja käytännössä. Samalla tulisi varmistaa periaatteiden leviäminen sekä julkiselle että yksityiselle taholle, etenkin niihin, jotka osallistuvat ja käyttävät profilointia. (Tietosuojavaltuutetun toimisto 17.2.2014.) Suosituksessa mainitaan, että vaikka profiloinnilla voidaan tuottaa asiakkaalle hyvää palvelua ja monenlaisia etuja, sitä voidaan käyttää myös esimerkiksi perusteettomasti estämään palvelunkäyttöä, mikä on tasa-arvoisuuden ja yksilön oikeuksien vastaista. Suosituksen perusteina mainitaan muun muassa, että profiloinnin tulee olla reilulla tavalla suoritettua, laillista ja perusteltuun käyttöön tarkoitettua. (Council of Europe 2010.) Euroopan komission vuonna 2012 tekemä ehdotus yleiseksi tietosuoja-asetukseksi on ollut valiokuntakäsittelyssä (viimeisin lausunto valmistunut 5.3.2015) (Oikeusministeriö 9.3.2015.) Tätä opinnäytetyötä kirjoitettaessa asia on siis vielä kesken.

Julkinen sektori käyttää profilointia muun muassa löytämään väkivaltarikoksiin taipuvaisia henkilöitä, veronkiertoon syyllistyviä verovelvollisia tai todennäköisesti erityisen tautiriskin omaavia potilaita (Heinonen 2001, 174). Kaupallisessa tarkoituksessa profilointia käytetään erityisesti palveluiden ja tuotteiden markkinoinnin apuna. Sen avulla markkinointiponnistukset voidaan kohdentaa tarkemmin, mikä parantaa markkinoinnin tehoa ja vähentää siitä aiheutuvia kus-

tannuksia. Sitä käytetään myös kuluttajien ohjaamisessa ja valvomisessa sekä tulevan ostokäyttäytymisen ennustamisessa. (Heinonen 2001, 172.)

Profiloinnin onnistumisen riskit liittyvät virheelliseen tai vanhentuneeseen tietoon sekä käytettyihin lähteisiin. Virheet yksittäisissä tietolähteissä voivat moninkertaistua lopullisessa profiilissa. Näiden riskien osittainenkin toteutuminen muodostaa profiilista epätarkan tai jopa valheellisen. Myös profiilin luomisessa käytetyt tiedonpoimintakriteerit ovat voineet olla epäkelpoja, niin ettei lopputuloksena syntyvä profiili vastaakaan sitä, mitä alun perin tarkoitettiin. (Heinonen, 2001, 180.) Sitä, miten profilointia tosiasiallisesti käytetään ja mitä tietoja sitä varten kerätään, on vaikea selvittää. Julkisen hallinnon suorittamasta profiloinnista ei ole tehty selvityksiä ja kaupallisista syistä tehdyt profiloinnit halutaan pitää esimerkiksi kilpailutekijöistä johtuen salassa. (Heinonen 2001, 172.)

Kun profiloinnin tekemistä varten kerätään ja analysoidaan tai muulla tavoin hyödynnetään tietoja, jotka voidaan liittää tiettyyn henkilöön kuuluviksi, kyse on henkilötietojen käsittelystä ja henkilötietolaki tulee sovellettavaksi. Henkilörekisterin tietoja ei saa käyttää profiloinnin suorittamiseksi, ellei sitä ole määritelty rekisterin käyttötarkoitukseksi. Asiakkaan tulisi myös olla tietoinen, mikäli hänen tietojaan profiloidaan suoramarkkinointitarkoituksiin. Asiakas on lähtökohtaisesti oikeutettu tarkistamaan mitä tietoja hänestä on talletettu. Tämä oikeus koskee myös profiloimalla luotua tietoa. (Vanto, J 2011, 28, 43, 123, 126.)

4.3 Esineiden internet

Esineiden internetillä (Internet of Things, IoT) tarkoitetaan järjestelmää, jossa esineet ja laitteet ovat vuorovaikutuksessa keskenään internetin välityksellä. Esineet ja laitteet tuottavat niihin asennettujen tunnistimien avulla erilaista tietoa ja niitä voidaan ohjata digitaalisesti. Esineiden internetiä on luotu pääasiassa yritys- ja teollisuuskäyttöä varten, mutta se laajenee koko ajan yhä enemmän myös kuluttajien käyttöön. Termillä ”esineiden internet” tarkoitetaan lähes samaa asiaa, kuin aiemmin käytetyllä käsitteellä m-to-m (machine to machine,

M2M), joka tarkoittaa koneiden ja laitteiden kytkemistä diagnostiikkaan tai ohjausjärjestelmään. (Tietosuoja 2015, 11–13).

Esineiden internetiä käytetään teollisuuden lisäksi esimerkiksi logistiikassa, terveyspalveluissa ja kiinteistönhoidossa. Sen avulla voidaan uudistaa ja tehostaa teollisten prosessien toimintaa ja valvontaa. Se avaa myös uusia mahdollisuuksia korkean teknologian tuotteiden tekemiseen ja niiden tuomiseen kaikkien ulottuville. IoT on jo osana tavallisen ihmisen arkea: etäluettavat sähkömittarit mahdollistavat sähkönkulutuksen ajantasaisen seurannan, ajotietokone tilaa huollon, navigaattori neuvoo parhaimman reitin kohteeseen ja rakennusten lämmitystä ja valaistusta säädetään sään ja käytön mukaan (kuvio 6). (Kotilainen, 2013).

Kuvio 6. Esineiden internet (Genco)

Kaiken sen hyödyn rinnalla, mitä esineiden internet yhteiskunnalle yleensä ja ihmisille yksilöinä tuottaa, on olemassa myös uhkansa. Esimerkiksi elektroniikkayritys Samsung on varoittanut asiakkaitaan valmistamastaan ääniohjattavasta älytelevisiosta, joka voi kuunnella huoneessa käytäviä keskusteluja ja lähettää ne eteenpäin kolmannelle osapuolelle (Helsingin

Sanomat 2015.) Mitään kovin henkilökohtaista tai arkaluontoista ei tällaisen television edessä kannata siis ääneen sanoa. Kuunteluominaisuuden tarkoitushan on, että televisio tunnistaisi vain sille suunnatut toimintakäskyt, kuten puhekomennoilla tehtävät internethaut.

Esineiden internetin myötä tapahtuvat muutokset ovat vasta alussa ja se tulee muuttamaan huomattavasti tapaamme toimia, työskennellä ja elää. Älykkäiden, keskenään viestejä ja tietoja vaihtavien koneiden määrän kodeissamme ennustetaan kasvavan kiihtyvällä nopeudella. Esimerkikkiyhdistelmä on sähkölaitteet ja ruokatavarat: jääkaappi ilmoittaa, mitä kaupasta on tarpeeen ostaa. Omatoimiseen terveydenhoitoon suunnitellut kellot voivat mitata verenpainetta ja veriarvoja tai kehitetään sovellus, jossa kaksi reseptilääkettä varoittavat potilasta mahdollisista haittavaikutuksista. (Tietosuoja 2011). Esineiden internet lähtee kuluttajatason tarpeista ja innovaatioista. Se perustuu nopeisiin ja edullisiin tapoihin välittää ja analysoida tietoa ja mahdollistaa uusien tuoteominaisuuksien syntymisen. Ne voivat liittyä esimerkiksi kuluttajalle tarjottuun oheistietoon tai parempaan käyttäjäkokemukseen. (Etla 2015, 42).

5 HENKILÖ- JA IDENTITEETTITIETOJEN VÄÄRINKÄYTÖN MUOTOJA

5.1 Identiteettivarkauksista yleisesti

Pelkistettynä identiteettivarkaus on sitä, että henkilö toisen henkilön tietoja käyttäen esiintyy hänenä rikollisessa tai muuten asiattomassa tarkoituksessa, esimerkiksi kiusan tekemiseksi, taikka saadakseen itselleen taloudellista hyötyä (Heinonen 2001, 202). Muut syyt identiteettivarkauksien tekemiseen liittyvät usein esimerkiksi huumeiden salakuljetukseen, laittomaan maahanmuuttoon, oikeuden pakoiluun, alaikäisten alkoholin käyttöön sekä muihin laittomuuksiin (Biegelman 2009, 113). Identiteettivarkaus on paljon vakavampi asia kuin yksittäisten henkilötietojen luvaton käyttöönotto. Henkilötietovarkaudessa menetetään joko yksittäisiä tai muutamia henkilötietoja, mutta identiteettivarkaudessa varastetaan ne tärkeimmät ja keskeisimmät henkilötiedot, joiden avulla voidaan sitten esiintyä eri palveluissa tai jopa viranomaisasioinnissa toisena henkilönä. (Rousku 2014, 16.)

Identiteettivarkauksilla on monta muotoa ja ne voidaan toteuttaa eri tavoin ja eri laajuuksissa. Identiteettivarkaus voidaan kohdistaa joko yhteen yksittäiseen henkilöön tai laajaan joukkoon ihmisiä, ja sen taustalla voi olla yksi henkilö tai järjestäytynyt rikollisryhmä. Se voidaan tehdä sekä reaalimaailmassa että internetissä. Yhteistä kaikille tapauksille on kuitenkin se, että identiteettitietoja kerätään ja käytetään oikeudetta joko hyödyn saavuttamiseksi tai vahingontuottamistarkoituksessa. Identiteettitieto voi olla henkilötunnus, osoite, luottokortin numero, sähköpostiosoite taikka tiliin tai palveluun liitetyt käyttäjätunnukset eli kaikki ne tiedot, jotka kohdentuvat tiettyyn henkilöön tai hänen oikeuksiinsa kirjautua tunnistusta vaativaan palveluun. (Sisäasiainministeriö 2010, 47–48, 50.)

Vuoteen 1999 saakka yksityishenkilön erehdyttäminen toisen passia, työtodistusta tai muuta vastaavaa dokumenttia käyttäen oli rikos, josta seurasi sakkorangaistus. Säännös kuitenkin poistettiin, eikä identiteettivarkaus ole tällä hetkellä Suomen laissa kriminalisoitu. Toisena henkilönä esiintyminen ei siis ole lainvastaista. Väärien henkilötietojen antaminen viranomaiselle sen sijaan on

rikos. Rikosoikeudelliseen vastuuseen joutuu myös silloin, kun identiteettivarkauden avulla tekee jonkin muun, rikoksen tunnusmerkit täyttävän teon esimerkiksi petoksen tai kunnianloukkauksen. (Forss 2014, 86.) Identiteettivarkauksien määrän yleistymistä onkin edesauttanut se, että lainsäädännössä ei ole määritelty sitä rikokseksi (Heinonen 2001, 201).

Kaikkeen henkilöihin liittyvään tiedon keräämiseen ja tallentamiseen liittyy yksityisyysongelmia. Yksityisyys puolestaan on monitahoinen ja laaja käsite. Yksityisyys on esimerkiksi poliittista, taloudellista, terveydellistä ja paikannustietoon liittyvää. (Liikenne- ja viestintäministeriö 2013, 5.) Yksityisyys voidaan myös käsittää ihmisen oikeutena pitää joitakin itseään koskevia asioita vain omana tietonaan (Järvinen 2010, 14). Taloudellisen yksityisyyden rikkomalla voidaan tehdä esimerkiksi petoksia. Terveydellisen yksityisyyden paljastaminen voi vaikuttaa uhrin vakuutussopimuksiin, työnsaantiin tai vain aiheuttaa kiusallisia tilanteita. Paikannustietojen perusteella viedään helposti henkilön anonymiteetti, koska sen avulla saadaan lyhyellä, muutaman päivän seurannalla yksilöityä suurin osa ihmisistä. (Liikenne- ja viestintäministeriö 2013, 5.) Massachusetts Institute of Technologyn (MIT) tekemän tutkimuksen mukaan esimerkiksi sosiaalisen median päivitysten ja korttimaksujen yhdistämisellä ihmisten identifiointi on helppoa. Tutkimuksessa käytiin läpi yli miljoonan erimaalaisen henkilön luottokorttimaksuja, jotka yhdistettiin sosiaalisen median päivityksiin. 90 % maksutiedoista pystyttiin kohdentamaan kortinhaltijaan vain neljän ostoajankohdan ja -paikan perusteella. (Viestintävirasto 2015, 45.)

Identiteettivarkauden mahdollistavia tietoja voidaan saada esimerkiksi kysymällä, löytämällä, huijaamalla ja varastamalla. Henkilökohtaisten ja luottamuksellisten tietojen saamista helpotetaan sosiaalisella manipuloinnilla (social engineering). Sanastokeskus TSK:n mukaan termi tarkoittaa ”*toimintaa, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä*” (TSK, tietotekniikan termitalkoot 2003). Sosiaalinen manipulointi on eri keinoin toteutettava vaikuttamiskeino, joka tähtää hyötymään ihmisen luontaisesta luottavaisuudesta ja ihmisen halusta auttaa toisia. Yhtenä keinona käytetään myös esimerkiksi sitä,

että toiselle voi syntyä pelko ongelmien syntymisestä. Aggressiivisuudella ja kiireen tunnun luomisella voidaan saada aikaan vaikkapa se, että henkilöllisyyden varmistaminen kestää liian kauan ja näin se sitten toteutetaankin nopeasti mutta huolimattomasti. Turvallisuusketjussa ihminen on se heikoin lenkki, ja juuri sitä taitavat manipuloijat käyttävät hyväkseen. Apuna käytetään vaihtelevia taivuttelu- ja suostuttelumenetelmiä, erilaisia vaikuttamistekniikoita sekä ihmisten vuorovaikutukseen vaikuttavia asenteita ja uskomuksia. Suoran toiminnan ja sosiaalisen manipuloinnin avulla haluttu tavoite voidaan saavuttaa paljon nopeammin kuin aikaa vievien teknisten ratkaisujen kautta yritettäessä. (Peltier, T 2014.)

Identiteettivarkaus voi kohdistua myös yrityksiin. Yhtä lailla pienet kuin suuretkin yritykset ovat vaarassa joutua identiteettivarkauden uhriksi. (Yle 25.7.2014). Euroopan petostentorjuntavirasto OLAF selvitti vuonna 2011 esimerkiksi sellaisen yritykseen kohdistuneen identiteettivarkauden, jossa kiinalainen tuotevalmistaja käytti Euroopan unionin alueella toimivan emoyhtiönsä nimeä hyväkseen kiertääkseen tullimaksuja. Euroopassa toimiva yhtiö toi Kiinasta tuotteita omaan myyntiinsä ohi emoyhtiön kirjanpidon. Kiinalainen tuotevalmistaja harhautti tullia esittämällä suurempia toimituseriä, kuin mitä eurooppalainen yhtiö oli todellisuudessa tilannut. Tällä toiminnalla saatiin yli miljoonan euron hyöty tullimaksuissa. (OLAF Euroopan petostentorjuntavirasto 2013, 4.)

Suomessa identiteettivarkauksien määrää ei ole voitu tilastoida, koska rikosten tilastointi perustuu rikosnimikkeisiin, eikä identiteettivarkautta kuvaavaa rikosnimikettä vielä ole rikoslaissa. Ainoa tapa selvittää asiaa olisi poimia identiteettivarkaudet käsin kaikista rikosilmoituksista. (Sisäasiainministeriö 2010, 48.) Oikeuspoliittinen tutkimuslaitos teetti kansallisen rikosuhritutkimuksen vuonna 2012. Tutkimukseen vastasi 7 746 henkilöä, iältään 15–74-vuotta. Vastaajista 1,4 % ilmoitti, että häneltä tai joltakin muulta hänen kotitalouteensa kuuluvalta oli varastettu identiteetti rikoksen suorittamiseksi. (Oikeuspoliittinen tutkimuslaitos 2013, s. 8,10.) Ylen aamu-tv:ssä 17.2.2014 kerrottiin poliisin arvion identiteettivarkauksien määrästä olevan noin 10 000/vuosi. (Yle 17.2.2014). Identi-

teettivarkauksien määrä on selkeästi kasvussa niin Suomessa kuin muuallakin maailmalla.

Internetin ja sosiaalisen median yleistyminen ovat kasvattaneet identiteettivarkauksien määrää nopeasti, vaikka valtaosa tapauksista ja niiden avulla tehdyistä kaikista väärinkäytöksistä ei tule koskaan esiin. Sosiaalisen median valeprofiileista tehdään Helsingin nettipoliisille ilmoituksia päivittäin. (Yle 25.7.2014.) Sähköiset palvelut ovat kasvattaneet suosiotaan, sillä niiden ansiosta palvelu on nopeampaa ja tarjonta monipuolisempaa. Verkkopalveluille on yhä ominaisempaa se, että palveluntarjoaja kerää tietoa käyttäjistä paitsi valvontatarkoitukseen myös profiloidakseen käyttäjiä. Tiedonkeruu on automaattista eikä käyttäjä useinkaan edes huomaa sitä. Tiedonkeruu perustuu asiakkaan tunnistamiseen, joten asioiminen anonyymisti onnistuu enää harvoin. (Heinonen 2006, 172–173.)

5.2 Identiteettivarkaus reaalimaailmassa

Tyypillisesti identiteettivarkaus toteutetaan käyttämällä henkilön kadottamia tai häneltä anastettuja asiakirjoja, kortteja ja tunnuksia. Näitä ovat esimerkiksi maksukortti, passi, ajokortti tai verkkopankkitunnukset. Haltuun otetun asiakirjan tai tunnusten avulla voidaan ottaa lainaa tai pikavippejä, ostaa tavaraa, tilata lehtiä, avata puhelinliittymiä ja tehdä muita sopimuksia. Pelkästään erilaisten, uhria identifioivien tietojen kerääminen ja niiden yhdistäminen mahdollistaa väärinkäytökset: selvittämällä henkilötunnuksen, osoitteen ja luottokortin numeron voidaan ostaa tavaroita ja palveluita internetin kautta. Lainaa tai tehtyjä ostoksia ei ole tarkoituskaan maksaa takaisin ja mikäli uhrin osoitetiedot on muutettu, voi mennä pitkäkin aika, ennen kuin petos tulee uhrin tietoon. (Heinonen 2001, 207.)

Pankki- ja luottokorttien skimmaaminen eli kopiointi on ollut identiteettivarkaiden käytössä jo vuosia. Kannettavalla kortinlukijalla kaapataan kortin magneettijuovalta kortin tiedot ja siirretään ne väärennetylle kortille, jota käytetään sitten taloudellisen hyödyn saavuttamiseksi. Skimmaamista on yleisesti käytetty ravinto-

loissa, huoltoasemilla ja sellaisissa paikoissa, joissa kortti viedään maksutapahtuman hoitamiseksi pois asiakkaan silmistä. Skimmauslaitteita on asennettu myös rahannostoautomaatteihin, jolloin kortin tiedot on luettu uhrin yrittäessä käteisnostoa. Pienen, automaatille asennetun kameran avulla on samalla saatu myös PIN-koodi. (Biegelman 2009, 36–37.) Kamera ei ole välttämätön, sillä tunnusluku saadaan napattua myös numeronäppäimistön päälle asennetulla valenäppäimistöllä (Nixu 2009). Suomessa skimmaaminen on hyvän yhteistyökulttuurimme, maantieteellisen sijaintimme ja etenkin sirukorttien käyttöönoton myötä lähes hävinnyt. Syyskuun loppupuolella vuonna 2014 epäiltyjä skimmaustapauksia oli vain yksi. Ulkomailla, varsinkin EU-alueen ulkopuolella ongelma on edelleen suuri ja Yhdysvalloissa yhä lisääntymässä. (Korttiturvallisuus 26.9.2014.)

Henkilön tunnistetietoja sekä tietoja henkilökohtaisista asioista, ostotottumuksista ynnä muusta, on sadoissa rekistereissä, kuten työpaikoilla, pankeissa, kaupoissa, vakuutusyhtiöissä, verovirastossa, Kelassa ja eläkeyhtiöissä. Työntekijät pääsevät tietoon käsiksi joko rajatusti tai kokonaan, joten jos epärehellinen työntekijä työskentelee jossakin näistä vaikka vain lyhyenkin aikaa, ehtii hän saada tietoja, joiden avulla väärän identiteetin luominen onnistuu. (Heinonen 2001, 213.) Esimerkiksi 24.3.2015 uutisoitiin kaupassa työskennelleestä miehestä, joka painoi muistiinsa hetkeksi haltuunsa ostotilanteissa saamiensa luottokorttien kaikki tiedot ja kirjasi tiedot paperille seuraavalla tauolla. Luottokorttitietoja käyttäen mies teki nettiostoksia ja pelasi uhkapelejä noin 30 000 eurolla. (MTV Uutiset 24.3.2015.)

Kaikkia identiteettivarkaudessa käytettäviä tietoja ei tarvitse edes varastaa. Paljon käytetty tapa on penkoa roskalaatikoita ja roskakoreja - sekä kotipihassa että työpaikoilla. Varsinkin kotioloissa harva tuhoaa asianmukaisesti pois heitettävää postia tai muita papereita, jotka kuitenkin voivat sisältää monia henkilöä koskevia yhteystietoja, asiakasnumeroita, tilinumeroita ynnä muita tietoja, joita sitten voidaan yhdistettynä käyttää vääriin tarkoitusperiin. (Heinonen 2001, 212.) Aktia Pankin tutkimuksen mukaan viisi prosenttia suomalaisista eli noin 250 000 ihmistä hävittää henkilötietoja sisältävät paperinsa heittämällä ne sel-

laisinaan roskiin tai paperinkeräykseen. Saman verran ilmoitetaan henkilötunnus internetin palveluissa, vaikka tarkkaa tietoa sen käytöstä ei tietojen antajalla olekaan. (Aktia Pankki 9.5.2014.)

Esimerkkitapaus: Helsinkiläinen Mirja sai syksyllä 2004 työsähköpostiinsa viestin Elloksen hänelle myöntämästä lainasta. Lainaa Mirja ei ollut hakenut, mutta viestissä esitetyt henkilökohtaiset tiedot olivat lähes täsmälleen oikein. Rahat oli tarkoitus siirtää tilille pankissa, jonka asiakas Mirja ei ollut koskaan ollut. Myöhemmin syksyllä poliisi pidätti väärillä henkilötiedoilla tiliä avaamassa olleen naisen. Naisen käyttämä tili täsmäsi siihen, jolle Mirjan nimissä haettu luotto oli tarkoitus siirtää. Kuulusteluissa nainen tunnusti päässeensä Mirjan kotitalon lukitulle sisäpihalle ja kaivaneensa roskapussista revittyjä papereita. Yhteistyössä kavereiden kanssa paperisilput oli selvitetty ja liimattu yhteen; näin saatiin kattavasti tietoa Mirjan henkilökohtaisista asioista: koko nimi, henkilötunnus, osoite, palkka ja jopa lasten lukumäärä. (Salminen J. 2010.)

Tietoja saadaan ihan laillisistakin lähteistä. Esimerkiksi rikosasioissa laaditut esitutkintapöytäkirjat, jotka ovat käräjäoikeuskäsittelyn alettua pääsääntöisesti julkisia, sisältävät asianosaisten henkilö- ja yhteystiedot (Kangasniemi 2012, 233). Myös kyseleminen on yleistä ja tietoja annetaan ihan vapaaehtoisesti. Tietojen hankkiminen uhrin lähipiiriin kuuluvilta on hyvin yleistä. Omaiset, ystävät ja työtoverit voivat antaa monenlaista tietoa vilpittömin mielin ilman epäilystäkään kyselijän motiiveista. (Heinonen 2001, 322.) Moni antaa salasanansa puolisolleen tai puoliso taikka muu perheenjäsen on voinut saada sen tietoonsa tahattomasti muuta kautta, esimerkiksi silloin, jos perheessä on säilytetty salasanoja yhteisesti samassa paikassa. Jos ihmissuhteessa tulee riitaa, tilanne voi kärjistyä salasanojen väärinkäytön kautta tehtävään kiusantekoon tai oman edun tavoitteluun. (Andersson–Koivisto 2013, 165.)

Joskus riittää yksi puhelinsoitto. Yle uutisoi tapauksesta, jossa prepaid-liittymällä ja tekaistulla sähköpostilla tilattiin iPhone ja iPad ja jätettiin laskut uhrin maksettavaksi. Tilaus onnistuu puhelimessa, koska tunnistaminen on jätetty tehtäväksi pakettia noudettaessa. Tavallinen Posti Group Oyj:n economy-

postipaketti voidaan kuitenkin luovuttaa lähetystunnusta ja kenen tahansa henkilöllisyystodistusta näyttämällä ja ainakin joskus henkilöllisyyden vahvistaminen jää tekemättä ja rikos onnistuu. (Yle-uutiset 17.10.2014.)

5.3 Identiteettivarkaus internetissä

Yhä useammin taloudellista hyötyä tavoittelevat identiteettivarkaudet tehdään internetissä, koska se on paljon helpompaa kuin reaalimaailmassa. Tietoverkossa suoritettavat rikokset voidaan automatisoida ja kohdistaa suurempaan ihmisjoukkoon, jolloin voidaan tavoitella mahdollisimman suurta taloudellista hyötyä mahdollisimman pienellä riskillä. Kiinnijäämisen riski onkin pieni, koska jäljet voidaan häivyttää käyttämällä sivullisilta kaapattuja internetliittymiä, anonyymiä välityspalvelinta tai TOR-verkkoa, jossa käyttäjän internetliikenne hajautetaan salattuna useisiin eri paikkoihin (Tor Project 2015). Rikosten tekemistä verkossa helpottaa myös se, että internet on maailmanlaajuinen, kun taas kunkin maan viranomainen on toimivaltainen vain omassa oikeuspiirissään. (Sisäasiainministeriö 2010, 53–54.) Digitaalisen identiteetin varastaminen on mahdollista heti, kun tunnistetiedot tavalla tai toisella on saatu tietoon (Heinonen 2001, 203).

Tietoverkossa tehtävistä maksukorttirikoksista yhä suurempi osa perustuu ajatukseen ”low value, high volume”. Tällä tarkoitetaan sitä, että suuri rikoshyöty koostuu suuresta massasta yksittäisiä, pieniä vahinkoja. Toisaalta tietojen automaattinen yhdistäminen ja tiedon laaja jakelu mahdollistavat myös suuremmat vahingot. (Sisäasiainministeriö 2010, 80, 83.) Etenkin verkossa tapahtuvia identiteettivarkauksia tehdäänkin puhtaasti kaupallisessa tarkoituksessa, niin että tiedot myydään eteenpäin vilpillisessä mielessä toimivien käytettäväksi (Kangasniemi 2012, 219).

Yksittäistapauksina internetissä tehtävät identiteettivarkaudet tavoittelevat usein kohdehenkilöön kohdistuvaa kiusantekoa. Kohteena voi olla esimerkiksi entinen puoliso, koulukaveri tai opettaja. Internetiin kirjoitettu viesti leviää nopeasti suu-

relle joukolle ja usein myös pysyvästi; tietoja on hyvin vaikea tai jopa mahdotonta jälkikäteen poistaa. (Sisäasiainministeriö 2010, 56.)

On myös muita internetissä tapahtuvia identiteettivarkauksia, joilla ei tavoitella taloudellista hyötyä eikä kohteena olevan henkilön loukkaamista, vaan kyseessä on lähinnä pilailu. Tällaisia ilmiöitä ovat valeprofiilien luomiset, jolloin tekijä rekisteröityy palveluun toisen, yleensä julkisuudenhenkilön nimellä taikka kirjoittaa kommentteja hänen nimissään. (Sisäasiainministeriö 2010, 57.) Toimintaa, jossa joku esiintyy verkkopalvelussa jonkun toisen henkilön nimissä ilman ilmeistä edunsaamistarkoitusta, kutsutaan myös identiteettivaltaukseksi (Aalto–Uusisaari 2009, 127). Motiivina voi olla myös osoittaa puutteita palvelinten turvallisuudessa esimerkiksi kaappaamalla salasanoja tai muita tunnisteita ja tuomalla tiedot esiin joko verkossa tai muulla tavoin. Muuta kiusantekoa on tapahtunut esimerkiksi niin, että kohdehenkilön nimissä on täytetty ilmoitus kirkosta eroamiseksi. (Sisäasiainministeriö 2010, 57.)

Nykyään iso osa ihmisten välistä viestintää tapahtuu sähköpostien ja sosiaalisen median kautta, joten näillä kanavilla käytettävien tunnusten merkitys on kasvanut (Viestintävirasto 2014, 4). Etenkin sähköpostipalveluiden kirjautumistunnukset ovat haluttuja, koska sähköpostien kautta voidaan saada selville henkilökohtaisten tietojen lisäksi kirjautumistietoja muihin palveluihin. Kun sähköpostin käyttäjätiedot ovat tiedossa, voidaan muiden palveluiden salasanoja selvittää monissa palveluissa olevan ”unohdin salasanani” -toiminnon kautta. (Andreasson–Koivisto 2013, 165.)

Tunnistetietoja voidaan selvittää erilaisten hakuohjelmien avulla, viranomaisten julkiset asiakirjat ovat vapaasti ja helposti käytettävissä, ja tietoja voi myös ostaa monilta web-sivustoilta ja palveluista. (Heinonen 2001, 204.) Henkilöön liittyviä tietoja voidaan selvittää myös internetiin siirrettyjen valokuvien ja niiden ”täggäyksen” avulla. Täggäämisellä tarkoitetaan toisen käyttäjän merkitsemistä omiin kuviin, paikkamerkintöihin tai tilapäivityksiin (Kansalaisyhteiskunta 2011). Valokuvissa näkyvät muut henkilöt, autojen rekisterinumerot, talojen numerot

ynnä muut voivat paljastaa henkilöstä yllättävän paljon (Valtiovarainministeriö 2010, 22).

Hakkeri on innokas tietokoneharrastaja, mutta termiä käytetään yleisesti myös henkilöstä, joka tunkeutuu oikeudettomasti tietoverkkoon tai tietojärjestelmään taikka käyttää niitä käyttöoikeuden vastaisesti. Tietojärjestelmiin murtautujaa kutsutaan myös nimellä krakkeri. (Sanastokeskus TSK 2004, 16.) Hakkereiden tai krakkereiden tekemistä tietomurroista uutisoidaan tämän tästä. Helmikuussa 2015 uutisoitiin sairausvakuutuksia myyvän Anthem -yhtiön joutuneen tietomurron kohteeksi Yhdysvalloissa. Yhtiön tietokannassa on 80 miljoonan ihmisen henkilötiedot, muun muassa syntymäajat, osoitteet ja tulot. Tietoturvayhtiö Cylancen toimitusjohtajan Stuart McCluren mukaan tiedot ovat aarreaitta kyberrikolliselle ja mahdollistavat erilaisia identiteettivarkauksia. (Helsingin Sanomat 5.2.2015.) Bloomberg Business -sivustolla tiedotettiin seuraavana päivänä todisteiden viittaavan teon olleen Kiinan valtion tukemien krakkereiden tekemä (MTV Uutiset 6.2.2015).

Verkkourkinnassa eli tietojenkalastelussa (engl. phishing) yritetään saada haltuun luottamuksellisia tietoja kuten esimerkiksi henkilötietoja, käyttäjätietoja ja luotto- ja pankkikorttitietoja. Urkinta tapahtuu yleensä sähköpostin kautta, mutta myös pikaviestejä käytetään. Tiedusteluviestejä lähetetään yritysten asiakaspalvelun tai viranomaisen, esimerkiksi poliisin nimissä, tai huijausviestit on voitu naamioida tarjoamaan jotain etuisuuksia. (Forss 2014, 108.) Aiemmin huijausviestit oli helpompi tunnistaa. Varoittavina merkkeinä oli muun muassa viesteissä käytetty huono suomen kieli ja epämääräinen ulkoasu. Nykyisin tietojenkalastajat ovat organisoituneet paremmin, toiminta on pitkäjänteisempää ja viestit huolella tehtyjä, aidon oloisia ja näköisiä. Huijauksissa käytetään apuna myös laadukkaasti tehtyjä, ulkoasultaan erehdyttävästi yritysten oikeiden nettisivujen tai verkkopankkisivujen näköisiä sivustoja. (Viestintävirasto 2014, 3, 5.) Tietojenkalastelu toteutetaan useimmiten massapostituksen kautta, mutta se voidaan kohdistaa myös yhteen tai tiettyihin henkilöihin tai organisaatioihin (Biegelman 2009, 38).

Smishing on matkapuhelimen tekstiviestien kautta tapahtuvaa tietojenkalastelua. Sana muodostuu sanayhdistelmästä phishing ja SMS (short message service) -tekstiviestijärjestelmä. Tekstiviestissä kohdehenkilö ohjataan asiallisilla ja pätevän kuuloisilla syillä verkkosivulle, joka tosiasiassa on huijaajan hallinnassa ja jossa pyritään kohdehenkilöä paljastamaan yksityisiä tietojaan. (Biegelman 2009, 37.)

Vishing puolestaan toimii niin, että kohdehenkilölle lähetetään ääniviesti pankin tai luottokorttiyhtiön edustajana. Viestissä vedotaan johonkin äärimmäisen tärkeään asiaan, joka olisi välttämätöntä hoitaa nopeasti. Asian hoitamiseksi annetaan puhelinnumero, joka on huijarin oma numero. Jos uhri soittaa numeroon, hänet ohjeistetaan näppäilemään tilinumero, PIN-koodi tai muita henkilökohtaisia tietoja. Huijari kerää ja tallentaa tiedot myöhempää, rikollista käyttöä varten. (Biegelman 2009, 38.)

Tietojenkalastelun kehittyneempi muoto on pharming eli liikenteen uudelleen ohjaus. Pharming eroaa phishingistä siten, että phishingissä suostutellaan käyttäjää antamaan salassa pidettäviä tietoja täysin vapaaehtoisesti kun taas pharmingissa otetaan käyttäjän tietokone hallintaan luvattomasti ilman, että käyttäjä edes huomaa sitä. Käyttäjän verkkopalvelujen käyttöä seurataan ja hänet ohjataan käyttämästään asiallisesta palvelusta tai sivustolta rikollisen hallussa olevaan palveluun tai sivustolle. (Andreasson–Koivisto 2013, 169.) Pharmingin tarkoituksena on selvittää käyttäjän kirjautumistunnisteita ja muita tietoja, joita tarvitaan pankkitilien tai palveluiden hyödyntämiseen etujen saavuttamiseksi. Pharmingia käytetään myös roskapostien lähettämiseen ja palvelunestohyökkäyksien tekemiseen. Näin hakkeri voi toimia salassa, sillä tekijä näyttää olevan koneen oikea haltija. (Andreasson–Koivisto 2013, 169.) Liikenteen uudelleenohjaus onnistuu murtautumalla huonosti suojattuun tai suojaamattomaan työasemaan ja muuttamalla sen nimipalveluasetuksia. Kun käyttäjä luulee kirjautuvansa esimerkiksi verkkokauppaan, yhteys ohjautuukin rikollisen hallussa olevaan palveluun ja käyttäjän näppäilemät kirjautumistunnisteet saadaan napattua. (Sisäasiainministeriö 2010, 55.)

Repäisevällä otsikolla tai muulla uteliaisuutta herättävällä tavalla voidaan käyttäjää erehdyttää niin sanottuun klikkauskaappaukseen (clickjacking). Siinäkään toteuma ei ole se, mitä alun perin luvataan, vaan käyttäjä voi klikkauksen myötä antaa toiselle esimerkiksi web-kameran käyttöoikeuden. Klikkauskaappauksen avulla voidaan myös syöttää käyttäjän koneelle haittaohjelmia, jotka kopioivat tietoja käyttäjän profiilista. Klikkauskaappauksesta käytetään Facebookissa myös nimeä tykkäämiskaappaus (likejacking). (Forss 2014, 119–120.)

Muita käytettyjä menetelmiä identiteettivarkauden tekemiseksi internetissä ovat näppäinpainallusten nauhoitus ja asiointiyhteyksien kaappaus. Syöttämällä haittaohjelman käyttäjän koneelle, voidaan kerätä internet-lomakkeiden näppäinpainalluksia. Näin rikollisen on mahdollista urkkia esimerkiksi luottokorttinumero tarkistetietoineen. Asiointiyhteyksien kaappaus on monimutkaisempaa ja vaatii kohdejärjestelmän hyvää tuntemista. Onnistuessaan se kuitenkin mahdollistaa esimerkiksi verkkopankeissa käytettävän kaksivaiheisen tunnistuksen murtamisen. (Sisäasiainministeriö 2010, 55.) Tietoja voidaan urkkia käyttäjän koneelta myös vakoiluohjelmien (Spyware) avulla. Kyseessä on ohjelma, joka kerää tietoja käyttäjän tietokoneelta ja välittää ne vakoilijalle. Yleensä vakoiluohjelmat ovat huomaamattomia, joten ne voidaan asentaa ja niitä voidaan käyttää ilman, että tietokoneen käyttäjä huomaa mitään. (Peltokorpi–Norppa 2015, 173.)

Yritykseen kohdistuva identiteettivarkaus internetissä voidaan toteuttaa esimerkiksi niin, että luodaan yrityksen toimintaa jäljittelevä www-palvelu, taikka toimitaan yrityksen edustajana sosiaalisessa mediassa. Näillä toimilla ei välttämättä saada taloudellista hyötyä, mutta sillä voi olla suurikin vaikutus yrityksen toimintaan tai sen julkisuuskuvaan. Useat tutkimukset osoittavat, että ihmiset hyväksyvät helposti omaan verkostoonsa sellaisia ihmisiä, joita he eivät tunne. Kun kuuluu verkostoon, on oikeutettu saamaan yksityiskohtaisempaa tietoa kuin muut palvelun käyttäjät. Jos tähän vielä yhdistyy liiallinen luottamus, osaamattomuus ja huolimaton toiminta, organisaation tietoturvariskit kasvavat. (Valtiovarainministeriö 2010, 15–16.)

Yrityksen identiteettivarkauden avulla voi tehdä myös petoksen esimerkiksi näillä kahdella tavalla: Rehellinen yrittäjä A myy rehelliselle yhtiö B:lle tuotteita. Huijariyhtiö C saa tästä tiedon. Se tekeytyy yrittäjä A:ksi ja ilmoittaa B:lle tilitietojensa muuttuneen ja antaa oman tilinumeronsa. Kun B maksaa laskun ostoksistaan, rahat menevät A:n sijasta C:lle. Huijariyhtiö C voi myös tekeytyä yhtiö B:ksi ja lähettää sen nimissä A:lle ilmoituksen, että B:n laskutusosoite on muuttunut. A lähettää laskun huijariyhtiö C:n ilmoittamaan postilokeroon. Huijarit muuttavat laskuun oman tilinumeronsa ja välittävät laskun eteenpäin B:lle. Taas kun B maksaa laskun ostoksistaan, rahat menevät A:n sijasta C:lle. Molemmissa tapauksissa rahat käy yleensä nostamassa bulvaani, henkilö, joka on kyllä rikollisten tuttu, mutta ei heille tärkeä. (Yle TV2, Poliisi-tv).

6 IDENTITEETTIVARKAUTTA KOSKEVA LAINSÄÄDÄNTÖ

6.1 Oikeus yksityisyyteen ja omiin tietoihin

Perustuslain 10 §:ssä on säädetty yksityiselämän suojasta (Perustuslaki 11.6.1999/731 2:10 §). Jokaisella henkilöllä on pääsääntöisesti oikeus hallita ja vallita omia henkilötietojaan ja päättää, miten niitä käsitellään. Oikeusturvan toteutumisen kannalta henkilöllisyyden suojaaminen on tärkeää myös internetissä ja sitä voidaan pitää kansalaisen perustavaa laatua olevana oikeutena (Valtioneuvosto 5.3.2009).

Myös Euroopan unionin perusoikeuskirjan mukaan jokaisella EU:n kansalaisella on oikeus siihen, että hänen yksityis- ja perhe-elämänsä, kotiaan ja viestejään kunnioitetaan (Euroopan unionin perusoikeusasiakirja 2. luku 7 artikla). Jokaisella on oikeus myös henkilötietojensa suojaan ja siihen, että hänen tietojaan käsitellään asianmukaisesti. Tietojen käsittelyn on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella taikka muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on myös oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuksi. (Euroopan unionin perusoikeusasiakirja 2. luku 8 artikla.)

Kuten aiemmin todettiin, yksityishenkilön erehdyttäminen toisen passia, työtodistusta tai muuta vastaavaa dokumenttia käyttäen oli rikos vuoteen 1999 saakka. Säännös kuitenkin poistettiin, koska pykälässä kuvattuun tekoon liittyi yleensä joku muu rikoksen tunnusmerkistön täyttävä teko. (Forss 2014, 86.) Asiaa käsiteltiin uudelleen vuonna 2006 rikoslain uudistamisen yhteydessä. Tuolloin ehdotettiin rangaistussäännöstä toiselle kuuluvan henkilötodistuksen väärinkäytöstä erehdyttämistarkoituksessa niin, että samalla annetaan ”oikeudellisesti merkityksellinen tieto”. Lakivaliokunta katsoi, että pelkkä toisen henkilötodistuksen käyttäminen ilman taloudellisen hyödyn tavoittelua tai asiakirjan väärentämistä ei ole sillä tavoin moitittavaa, että sitä olisi syytä ottaa rikoslaissa rangaistavaksi. Valiokunta huomautti myös, että käytännössä ehdotuksen toteuttaminen tulisi kohdistumaan vain alaikäisiin ja että ehdotus on suhteelli-

suusperiaatteen vastainen. Lopputulos siis oli, että kriminalisoinnille ei katsottu olevan riittäviä perusteita. Kriminalisointiperiaatteeseen kuuluu, että sille on oltava hyväksyttävä peruste ja painava yhteiskunnallinen tarve ja sen tulisi olla ennaltaehkäisevää. Lisäksi rikosoikeudellisen laillisuusperiaatteen mukaan tunnusmerkistön tulee olla täsmällinen ja tarkkarajainen. (Lakivaliokunnan mietintö 15/2005 vp.)

6.2 Identiteettivarkauden rikosoikeudelliset seuraamukset

Perinteisten tunnistamisasiakirjojen, kuten passi, ajokortti ja henkilökortti, avulla tehdyt identiteettivarkaudet tulevat tyypillisesti ilmi väärennysrikoksina (Rikoslaki 33 luku) tai petosrikoksina (Rikoslaki 36 luku). Toisena henkilönä esiintymistä toiselle yksityishenkilölle ei ole Suomen laissa kriminalisoitu, sen sijaan viranomaiselle on lainvastaista esiintyä muuna kuin itsenään. Viranomaisen erehdyttämisestä tällä tavoin voidaan tuomita väärän henkilötiedon antamisesta viranomaiselle (Rikoslaki 16:5 §), rekisterimerkintärikoksesta (Rikoslaki 16:7 §) tai väärän todistuksen antamisesta viranomaiselle (Rikoslaki 16:8 §). (Sisäasiainministeriö 2010, 53.)

Rikokset, joissa ei tavoitella taloudellista hyötyä, vaan tarkoitus on ainoastaan vahingoittaa kohdetta, voivat täyttää kunnianloukkauksen (Rikoslaki 24:9 §) tai yksityiselämää loukkaavan tiedon levittämisen (Rikoslaki 24:8 §) tunnusmerkistön (Sisäasiainministeriö 2010, 56). Esimerkiksi Facebook -yhteisöpalvelimelle voidaan helposti luoda valeprofiili toisen henkilön nimissä. Näissä tapauksissa ongelmaksi on noussut se, että vaikka kunnianloukkauksen tai yksityiselämää loukkaavan tiedon levittämisen tunnusmerkistö täyttyisikin, jäävät rikokset pääsääntöisesti selvittämättä, koska tekijän IP -osoitteen saaminen Yhdysvalloissa sijaitsevalta palvelimelta on lähes mahdotonta. (Sisäasiainministeriö 2010, 57.) Toisen henkilön käyttäjätilin kaappaaminen voi täyttää tietomurron tai viestintäsalaisuuden loukkauksen tunnusmerkistön, vaikka sen avulla ei mitään toimenpiteitä tekisikään. Jos sen avulla uhkaillaan tai loukataan, voi teko tulla tuomittavaksi laittomana uhkauksena tai kunnianloukkauksena. (Forss 2014, 93.) Kiusaamistarkoituksessa tehtyjen identiteettivarkauksien avulla tehdyt seuranhakuilmoitukset tai myynti-ilmoitukset voivat aiheuttaa valtavan määrän yh-

teydenottoja. Tämä voi tulla tutkittavaksi välillisenä viestintärauhan rikkomisena. (Forss 2014, 95.)

6.3 Identiteettivarkauksia koskevaan lainsäädäntöön tulossa olevat muutokset

Identiteettivarkauksien määrän kasvun myötä kasvoi uudelleen myös yleinen keskustelu kyseisen toiminnan kriminalisoinnin tarpeesta. Kirjallisen kysymyksen identiteettivarkauden rangaistavuudesta ovat esittäneet ainakin Suomen Keskustan Antti Kaikkonen (KK 739/2010 vp) ja Kansallisen Kokoomuksen Outi Mäkelä (KK 855/2012 vp). Identiteettivarkauksien kriminalisointitarvetta selvitti sisäasiainministeriön asettama henkilöllisyyden luomista koskevaa hanketta käsittelevä työryhmä kahden vuoden ajan. Työryhmä julkaisi loppuraporttinsa 15.12.2010. Työryhmän mielestä kansalaisia tulisi suojata identiteettivarkauksilta ja ainakin niiden vaikutuksilta, koska teoilla voidaan loukata useita eri perusoikeuksia. Rikosoikeudellinen säädäntä ei olisi tarpeen perinteisten, reaalimaailmassa tapahtuvien tekojen osalta, mutta tietoverkossa tapahtuvien rikosten aiheuttama vahinko on niin suuri ja toimivaltuudet niiden tutkimiseen reaalimaailmaa vähäisemmät, joten verkkorikosten osalta olisi tarpeen paitsi rikosoikeudellinen säätäminen myös muiden, rikoksia ennaltaehkäisevien toimien käyttö. (Sisäasiainministeriö 2010, 75.)

Valtioneuvosto antoi 7.3.2013 periaatepäätöksen järjestäytyneen rikollisuuden torjunnan strategiasta. Tuolloin hallitusohjelmassa todettiin, että järjestäytyneen rikollisuuden torjuntaa tehostetaan ja uuden erityislain tarvetta selvitetään. Osana järjestäytyneen rikollisuuden torjuntaa panostetaan myös tietoverkkorikollisuuden torjuntaan. Euroopan unionin laajenemisen ja vapaan liikkuvuuden myöstä Suomeen on tullut uusia, kansainvälisesti toimivia järjestäytyneitä rikollisryhmiä. Strategian tavoitteena onkin ollut järjestäytyneen rikollisuuden toimintaedellytysten heikentäminen ja ehkäiseminen niin, että sen määrä vähentyisi (Valtioneuvosto 2013.)

Oikeusministeriön arviomuistiossa 15.3.2013 todetaan identiteettivarkauden olevan käsitteenä epämääräinen ja sen sisältävän eri yhteyksissä erilaisia teko-

ja ja ongelmia. Se on myös oikeudellisesti sangen epäselvä. Identiteettivarkaudet tulisi kuitenkin ottaa vakavasti huomioon nykyisessä yhteiskunnassa, joka perustuu yhä enemmän tietoverkkoihin. Ongelmaksi muistio nostaa sen, että miten pelkkä toisena henkilönä esiintyminen ilman taloudellisen vahingon tuottamista taikka loukkaamatta toisen kunniaa ja yksityisyyttä olisi vahingollista, ja siten perusteltua säätää rangaistavaksi. Kriminalisointiperiaatteeseen kuuluu tekstissä aiemmin mainittujen perusteiden lisäksi se, että teko pitää voida kuvata niin yksilöidysti, että kielletty teko on erotettavissa laillisesta teosta. Rikosoikeutta koskee myös ultima ratio -periaate eli sitä tulisi käyttää vasta viimesijaisena keinona. (Oikeusministeriö, arviomuistio 15.3.2013.)

12.8.2013 on annettu Euroopan parlamentin ja neuvoston direktiivi, joka koskee tietojärjestelmiin kohdistuvia hyökkäyksiä. Tietoverkkorikollisuutta ovat esimerkiksi tietomurrot, palvelunestohyökkäykset ja identiteettivarkaudet. Niiden katsotaan olevan erityisesti järjestäytyneeseen rikollisuuteen liittyvänä kasvava uhka sekä Euroopan unionissa että maailmanlaajuisesti. Tietoliikennerikokset tulevat olemaan entistä vahingollisempia, laajamittaisia ja toistuvia. Niillä on rajaylittävä vaikutus, joten yhtenäiset käytännöt ja yhteistyö jäsenmaiden välillä ovat tärkeitä. Myös rikostunnusmerkistöjen osalta on luotava yhteinen linja. Yhtenä direktiivin tavoitteena on henkilöllisyysvarkauden ja muiden henkilöllisyyteen liittyvien rikosten estäminen. Direktiivissä säädetään, että jäsenvaltioiden on kansallisissa laissaan varmistettava, että määriteltyjen rikoksien, joihin liittyy toisen henkilön henkilötietojen väärinkäyttö siten, että se harhauttaa kolmatta osapuolta ja aiheuttaa vahinkoa henkilöllisyyden oikealle omistajalle, katsotaan raskauttavaksi asianhaaraksi. Tällaisia rikoksia ovat esimerkiksi laiton järjestelmän häirintä ja laiton datan vahingoittaminen. (Euroopan unionin virallinen lehti 14.8.2013.)

Suomen lainsäädännössä ei tällä hetkellä ole säännöstä identiteettivarkaudesta tai identiteetin väärinkäytöstä. Direktiivin toimeenpanemiseksi hallitus on tehnyt eduskunnalle lakiesityksen eräiden tietoverkkorikoksia koskevien säännösten muuttamiseksi ja eräiksi siihen liittyviksi laeiksi. (HE 232/2014 vp.) Esityksessä ehdotetaan, että rikoslain 38 lukuun lisätään uusi, identiteettivarkautta koskeva

pykälä 9b. Ehdotuksen mukaan ”*Identiteettivarkaudesta tuomittaisiin se, joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee*”. Teon seuraamukseksi ehdotetaan sakkorangaistusta. Pykälässä tarkoitettu ”toinen” voi olla myös oikeushenkilö. Erehdytetty kolmas osapuoli voi olla joko henkilö taikka henkilöiden luoma tai ylläpitämä tietojärjestelmä. ”Taloudellinen vahinko” tarkoittaa esimerkiksi tapauksesta johtuvia selvittelykuluja ja ”haitta” selvittämisestä johtuvaa vaivannäköä. Ehdotuksella tavoitellaan identiteettivarkauden uhrin asianomistaja-aseman selkeyttämistä. (HE 232/2014 vp.) Eduskunta hyväksyi lakiehdotuksen ja asian käsittely päättyi 10.3.2015. Laki tulee voimaan 4.9.2015, jolloin direktiivi on pantava jäsenvaltioissa täytäntöön. (Eduskunta 10.3.2015.)

7 IDENTITEETTIVARKAUDELTA SUOJAUTUMINEN JA VAHINKOJEN MINIMOIMINEN

7.1 Henkilön suojautumiskeinot

Henkilöllisyyden turvaaminen ja itsemääräämisoikeuden toteutuminen on olennaisen tärkeä asia sekä fyysisessä että sähköisessä toimintaympäristössä. Palveluntuottajien ja muiden toimijoiden vastuuseen kuuluu osaltaan käyttäjän identiteetin suojeleminen. Suuri vastuu on kuitenkin myös käyttäjällä itsellään. (Sisäministeriö 20.4.2011).

Perusohje identiteettivarkaudelta suojautumiseen on huolellisuus henkilötietojen ja niitä sisältävien dokumenttien käsittelyssä. Kaikki asiakirjat tulee säilyttää ja hävittää huolella. Erityistä huolellisuutta kannattaa noudattaa kaikissa pankki- ja rahoitustapahtumia sisältävissä papereissa. Pois heitettävät asiakirjat ja tunnistetietoja sisältävä posti kannattaa silputa ja mielellään vielä hajauttaa eri roskaeriin, tai mieluiten polttaa, mikäli se on mahdollista. (Verkkouutiset 8.2.2015.)

Verkossa tapahtuvissa huijausyrityksissä käytetään perinteisiä psykologisia keinoja. Niissä vedotaan ihmisten toiveisiin ja tunteisiin tai auktoriteetteihin. Huijausten ehkäisemiseksi kannattaa käyttää niin sanottua maalaisjärkeä. Jos tarjous kuulostaa liian hyvältä, se harvoin on totta tai jos asia tuntuu epäilyttävältä, se yleensä on sitä. Toisinaan kannattaa jäädä hetkeksi miettimään, miksi juuri minua lähestytään, mitä tietoja minulta halutaan ja miten ne liittyvät itse asiaan? Mitä riskejä on siitä, että toimin kehotuksen mukaisesti? Pikaiseen päätöksentekoon vetoaminen esimerkiksi lyhyellä tarjous- tai vastausajalla on vanha keino, jolla pyritään käyttäjän harkinnan pettämiseen. (Kilpailu- ja kuluttajavirasto 7.5.2014.)

Henkilötunnusta ja muita henkilötietoja annettaessa kannattaa käyttää harkintaa ja tehdä se vain siinä tapauksessa, että tiedonsaaja on ehdottomasti luotettava. Verkkopankissa käytettävää salasanaa ja siihen liittyvää tunnuslukulistaa ei kannata pitää mukana eikä niitä pidä säilyttää samassa paikassa. Pankki- tai

luottokorttiin liittyvää tunnuslukua ei saa säilyttää kortin yhteydessä. Varminta olisi, että pysyvät salasanat olisivat vain omassa muistissa. Tunnuslukua käytettäessä tulee aina varmistua turvallisesta asioinnista. Tunnusluvun näppäily kannattaa tehdä toisen käden suojassa tai muuten sillä tavoin, ettei kukaan ulkopuolinen pääse näkemään näppäiltävää lukua. (FINE, turvallisuus ja tietosuoja.)

Luottokortti- tai muita maksutietoja ei pidä antaa tuntemattomille eikä etenkään puhelimitse. Verkko-ostoksissa kannattaa valita luotettaviksi todetut ja turvalliset verkkokaupat. (Tietosuoja 2010, 3.) Ostaminen verkkokaupasta luottokorttia käyttäen on turvallista, kun yhteys on suojattu. Merkkinä suojatusta yhteydestä on nettisivun osoitekentässä oleva lukko -tunnus ja osoitteen muoto on https://. (Ficom 2011, Turvallisesti netissä.)

Maksunvälityspalvelu tekee luottokorttimaksamisesta turvallisempaa toimimalla asiakkaan ja kauppiaan välissä siten, että asiakkaan luottokortin tiedot eivät koskaan päädy kauppiaalle. Asiakas luo itselleen tilin palvelusivustolla ja tallentaa sinne luottokortin tiedot, käyttäjätunnuksen ja salasanan. Tämän jälkeen maksunvälityspalvelua voi käyttää sellaisissa verkkokaupoissa, jotka ovat mukana järjestelmässä. Esimerkki tällaisesta maksunvälityspalvelusta on amerikkalainen PayPal -palvelu. (Järvinen 2010, 97.)

Sähköpostiviestien suhteen kannattaa olla tarkka: niitä ei kannata avata eikä niihin vastata, mikäli ne vaikuttavat epäluotettavilta (Tietosuoja 2010, 3). Erilaisiin nettiarvontoihin, kyselyihin ja mainoskampanjoihin kannattaa suhtautua kriittisesti ja harkita, antaako niissä yksityiskohtaisia tunnistetietojaan. Kaikkia linkkejä ja liitetiedostoja ei todellakaan kannata avata; niiden takaa voi koneelle latautua haittaohjelmia, jotka mahdollistavat tietokoneen etähallinnan ja käytön rikollisiin tarkoituksiin. (Forss 2014, 102.) Haittaohjelmia on erityyppisiä, kuten esimerkiksi madot, virukset, troijalaiset sekä vakoilu- ja kiristysohjelmat. Ne toimivat toisistaan poikkeavilla tavoilla ja niillä on eri tavoitteet. Yhteistä niille kuitenkin on joko vahingon aiheuttaminen tai järjestelmän hyväksikäyttäminen laittomasti. (Limnéll ym 2014, 236.)

Tietokoneen käyttöjärjestelmä, ohjelmistot ja selaimet kannattaa pitää päivitettynä sekä virustorjunta ja palomuuri ajan tasalla. Myös matkapuhelimessa olevat tietoturva-asetukset kannattaa ottaa käyttöön. Eri palveluissa kannattaa käyttää eri salasanoja. (Forss 2014, 101.) Mikäli mahdollista, kannattaa verkkoasioinnit erotella niiden tärkeyden perusteella ja hoitaa verkko-ostokset, verkkopankki- ja viranomaisasiointi eri päätelaitteelta kuin viihdekäyttö ja muu verkkoviestintä ja –selailu (Sisäasiainministeriö 2010, 78).

Salasanan laatuun tulee kiinnittää erityistä huomiota. Hyvä salasana on riittävän pitkä (vähintään 10 merkkiä) ja siinä käytetään sekä isoja että pieniä kirjaimia, numeroita ja erikoismerkkejä. Salasana tulee vaihtaa säännöllisesti, esimerkiksi kolmen kuukauden välein, eikä entistä salasanaa kannata ottaa enää uudelleen käyttöön. (Rousku 2014, 179.)

Erilaiset yhteisöpalvelut, kuten esimerkiksi Facebook ja MySpace, ovat palveluita, joille käyttäjät luovat omia sisältöjään ja niissä julkaistaan paljon omaan elämään liittyviä asioita. Yksityisasetuksia muokkaamalla voidaan määrittää, kuinka laajasti tiedot näkyvät toisille käyttäjille. Silti on hyvä muistaa, että kaikki julkaisut voivat levitä kavereiden kautta laajalle joukolle ihmisiä. Kannattaa siis harkita myös kaveripyyntöjen hyväksymistä. (Forss 2014, 101.)

Omat luottotiedot kannattaa tarkistaa aika ajoin. Lakisääteisesti jokaisella henkilöllä on oikeus tarkistaa omat luottotietonsa maksutta kerran 12 kuukaudessa joko käymällä Asiakastiedon kuluttajaneuvonnassa tai lähettämällä kirjallisen tarkistuspyynnön (Suomen Asiakastieto 2015, Tietoa luottotiedoista). Asiakastieto Oy:llä on myös maksullinen Omatieto -palvelu, jonka kautta saa tiedon aina, kun omia luottotietoja käytetään tai niistä tehdään kyselyitä. Palvelun avulla voi siis seurata omia luottotietoja säännöllisesti. (Suomen Asiakastieto 2015, Omatieto -palvelu.) Myös mySafety myy identiteettivarkauden suojaksi tietovahtipalvelua ja sen myymästä ID-turvasta korvataan taloudellisia vahinkoja 10 000 euroon asti (mySafety Oy 2015, ID-Turva).

Suomen Asiakastieto Oy on Suomen suurin yritys- ja luottotietoyhtiö, joka toimii yhteistyössä maailman johtavien luottotietoyritysten kanssa. Sen kautta voidaan asettaa ”Oma Luottokielto” -merkintä. Merkinnän tekeminen ei täysin estä henkilötietojen väärinkäyttöä luottosopimuksissa, mutta sillä voidaan merkittävästi pienentää riskiä, vähentää vahinkoja ja välttää henkilötietojen väärinkäytöstä aiheutuvaa selvitystyötä. Kun luottokieltomerkintä on tehty, se on luotonmyöntäjällä nähtävissä Asiakastiedon rekisteriin tehtävässä luottotietokyselyssä. Luottotiedot tarkistetaan monissa päätöksentekotilanteissa kuten luotonmyönnössä, osamaksusopimuksissa, puhelinliittymien avauksessa ja asunnon vuokrauksessa. Kun Oma luottokielto -merkintä on tehty, asianomaisen on todistettava oikeellisuutensa saamallaan virallisella todistuksella. Palvelu on maksullinen. (Suomen Asiakastieto Oy 2015, Oma luottokielto.)

Perinteisistä suomalaisista vakuutusyhtiöistä Aktia Pankki myy vakuutusta identiteettivarkauksien varalle. Laajaan kotivakuutukseen kuuluva vakuutus henkilöllisyysvarkauden varalta korvaa juridisesta avusta aiheutuvia kohtuullisia ja välttämättömiä kustannuksia, mutta ei muita varkaudesta aiheutuvia taloudellisia tappioita, kuluja tai kustannuksia. Uhria myös autetaan selviytymään rikoksesta aiheutuneista ongelmista joko neuvomalla tai huolehtimalla asioista vakuutetun puolesta. (Aktia Pankki. Kotivakuutus, vakuutusehdot 1.1.2015 alkaen, 17.)

7.2 Huomioitavia tietoturva-asioita työpaikalla

Yrityksissä ja muissa organisaatioissa tulee ohjauksen ja koulutuksen avulla neuvoa työntekijöitä myös identiteettivarkauksien uhkien varalta. Huomioita kannattaa kiinnittää ainakin siihen, miten verkkoidentiteettiä käytetään ja mitä organisaatiosta ja sen toiminnasta on lupa kertoa. Huolellisuutta verkostoiduttaessa ja kontaktien hyväksymisessä, käyttöehtojen hyväksymisessä ja salasanojen käytössä on syytä korostaa. Ohjelmistoissa olevat yksityisyyden suoja-asetukset kannattaa säätää tarvittaessa oletusarvoja tiukemmiksi. Varoittaminen kalasteluviesteistä ja kolmannen osapuolen sovelluksista ja niihin mahdollisesti liittyvistä riskeistä sekä kehotus harkinnan käyttämisestä on hyvää turvalli-

suusriskien toteutumisen ennaltaehkäisemistä. (Valtiovarainministeriö 2010, 28–29.)

IT-tukea antava tai tarjoava mikrotukihenkilö ei koskaan kysy salasanaa puhelimessa. Siihen ei ole tarvetta, sillä henkilöllä, jonka tehtäviin oikeasti yrityksen tuki- ja ylläpitotehtävät kuuluvat, on omat järjestelmänvalvojan tunnukset, joiden avulla hän pääsee näkemään tarvittavat tiedot ja/tai tekemään tarvittavat muutokset. (Aalto–Uusisaari 2009, 126.)

Työpisteissä toteutettavalla tietoturvalla ehkäistään tietojen joutuminen vääriin käsiin. Vakiintuneeksi käytännöksi kannattaa ottaa tietokoneen lukitseminen aina sen äärestä poistuttaessa. Koneeseen voi asentaa myös automaattisen lukituksen, joka tulee käyttöön, kun tietokonetta ei säädettynä aikana (esimerkiksi viisi–kymmenen minuuttia) ole käytetty. Kannettavissa tietokoneissa on suositeltavaa käyttää suojakalvoa, jolloin ohikulkijat eivät pysty näkemään näytöllä olevaa materiaalia. Työpaikalla tulee huolehtia, että tieto osataan luokitella oikealla tavalla. Kaikki salassa pidettäviä tietoja sisältävät paperit tulee säilyttää lukitussa tilassa. Kun tietoa välitetään muualle, tulee varmistua siitä, että vastaanottajalla on oikeus saada annettava tieto ja että se välitetään oikeaan kohteeseen (esimerkiksi faksin numero tulee varmistaa). Lisäksi tulee huolehtia, että se toimitetaan tietoturvallisella tavalla. Tarpeettomat asiakirjat ja tiedostot tulee hävittää asianmukaisesti. (Rousku 2014, 163–165.)

7.3 Identiteettivarkauden seuraukset ja jälkitoimenpiteet

Identiteettivarkauksien ja muiden henkilötietojen väärinkäytön pääasiallinen tarkoitus on joko tuottaa tekijälleen taloudellista hyötyä taikka aiheuttaa vahinkoa varkauden kohteelle. Pääsääntöisesti uhri tulee tietoiseksi tapahtuneesta vasta jälkikäteen, joskus hyvinkin pitkän ajan kuluttua. Mikäli identiteettivarkauden ohessa on tehty uhrin nimissä osoitteenmuutos, ohjautuvat laskut muun postin ohessa muualle. Tämäkin hidastaa rikoksen ilmituloa. Toiseksi henkilöksi voidaan tekeytyä myös siksi, että jostakin syystä halutaan peittää oma, todellinen

henkilöllisyys. Tällöin uhri ei välttämättä tule koskaan tietämään kaikkia hänen nimissään tehtyjä väärinkäytöksiä.

Identiteettivarkauden avulla tehdyt ostot, tilaukset ja pikavipit tuottavat taloudellista menetystä uhrilleen. Rahaa saadaan uhrin nimissä myös varastettujen korttien tai pankkitunnusten avulla. Taloudellinen menetys voi jäädä pysyväksi. Taloudelliset menetykset voivat johtaa myös negatiivisiin luottotietomerkintöihin, jonka seurauksena esimerkiksi lainan saanti tai matkapuhelin liittymän avaaminen vaikeutuu tai käy jopa mahdottomaksi. Uhrin elämää voi hankaloittaa myös se, että hän laittaa itse itselleen luottokieltomerkinnän enempien rikollisen tekemien vahinkojen välttämiseksi.

Nimen ja maineen menetyksiä voi myöhemmin olla mahdotonta korjata koskaan täysin. Reaalimaailmassa väärinkäytökset voidaan saada loppumaan, kun väärinkäytetty henkilöllisyyspaperi saadaan pois rikollisen hallusta. Verkossa sen sijaan rikollisen toiminnan estäminen on paljon vaikeampaa. Sekä identiteettivarkauden selvittäminen että väärien tietojen poistaminen on ongelmallista ja aikaa vievää. Kannattaa kuitenkin mahdollisimman tarkoin yrittää selvittää kaikki ne tahot, joissa henkilötietoja on väärinkäytetty ja ilmoittaa asiasta näille tahoille. Verkossa tapahtuvaa rikosta voi olla erityisen vaikea selvittää, koska sen tekijä voi toimia mistä päin maailmaa tahansa tai rikolliset voivat tehdä yhteistyötä tapaamatta tai edes tuntematta toisiaan. Todisteet teosta voivat olla hajallaan, esimerkiksi useilla eri ulkomaisten palveluntarjoajien tietojärjestelmissä. Väärää tietoa sosiaalisesta mediasta ei välttämättä koskaan saada kokonaan poistettua, koska joku tiedon saanut henkilö on voinut tallettaa sen omiin tiedostoihinsa ja laittaa esille uudelleen joskus myöhemmin. Varkaudesta aiheutuvia sosiaalisia seuraamuksia uhrille ja hänen lähipiirilleen onkin vaikea mitata, mutta varmasti se tuottaa uhrilleen aina mielipahaa.

Tärkeää olisi yrittää pysäyttää henkilötietojen väärinkäytön jatkuminen mahdollisimman nopeasti. Tulevia laskuja, luottokorttimaksuja ja tiliotteita kannattaa seurata tehostetusti ja kaikki maksutiedoissa ilmenevät epäselvyydet selvittää välittömästi. Myös puhelu- ja viestintätietoja on hyvä seurata normaalia tar-

kemmin. Luottotiedot kannattaa myös tarkistaa heti, jotta mahdollisimman varhaisessa vaiheessa tulee tietoiseksi mahdollisista häiriöistä. Mikäli kortit ovat kadoksissa, tehdään ilmoitukset pankille ja/tai luottokorttiyhtiölle korttien sulkemiseksi. Pankkitunnusten katoamisesta ilmoitetaan myös joko pankkiin tai pankin aukioloajan ulkopuolella sulkupalveluun tunnusten sulkemiseksi. Myös henkilöllisyyspapereiden katoamisesta ilmoitetaan, koska silloin käteisnostot tai muut tunnistamista vaativat asioinnit kadoksissa olevalla asiakirjalla ei onnistu. Mikäli kyse on varkaudesta, tehdään ilmoitus myös poliisille. Jos kyseessä on tietokoneella tapahtunut huijaus, kyseistä tietokonetta ei kannata käyttää pankki-asiointiin eikä muihin tärkeisiin palveluihin, ennen kuin laitteiston tietoturva on varmistettu. Kaikki sellaiset tunnukset ja salasanat, joiden epäilee olevan toisen henkilön tiedossa, pitää vaihtaa välittömästi. Mikäli tulee tietoiseksi jossakin henkilörekisterissä olevista vääristä tiedoista, pyydetään rekisterinpitäjää oikaisemaan tiedot ja poistamaan virheelliset merkinnät.

8 REKISTERINPITÄJÄN VELVOLLISUUS HUOLEHTIA TIETOTURVASTA

8.1 Fyysinen tietoturva

Tietoturva voidaan käsittää tietojen ja niiden käsittelyyn liittyvien laitteiden ja toimintaympäristön suojaamista siten, että tietojen luottamuksellisuus, eheys ja käytettävyys on turvattu (Pitkänen ym. 2013, 215). Henkilötietojen lainmukaisessa ja turvallisessa käsittelyssä toimintaympäristö on olennainen osa, kun pyritään varmistamaan se, että tietoja pääsevät näkemään ja niitä käsittelemään vain ne, joilla on siihen oikeus. Rekisterinpitäjän tulee huolehtia siitä, että laitteisto, jolla henkilötietoja käsitellään, on suojattu viruksia ja ulkopuolisia hyökkäyksiä vastaan. Ajantasaiset virustorjunta- ja palomuurijärjestelmät sekä tietoliikenteen tapahtumien kerääminen tapahtumalokiin ovat osaltaan edistämässä asianmukaista henkilötietojen käsittelyä (Valtiovarainministeriö 2012, 43.) Myös se, että tietoja sisältävät tallennusvälineet kuten kiintolevyt on suojattu ja varmistettu laiterikkojen tai vaikkapa tulipalon varalta, on osa henkilötietolaissa määrättyä velvollisuutta tietojen huolellisessa säilyttämisessä (Henkilötietolaki 523/1999 7:32 §). Tiedon suojaaminen tapahtuu sekä teknisin ratkaisuin, että hallinnollisin prosessein (kuvio 7).

Kuvio 7. Organisaatiossa käsiteltävän tiedon turvaaminen (Valtiovarainministeriö 2012,13)

Fyysiseen tietoturvaan sisältyy tietojärjestelmien rakentaminen siten, että niihin pääsevät käyttäjiksi ainoastaan sellaiset henkilöt, joilla on tehtäviensä puolesta tarve käsitellä kyseisiä tietoja. Järjestelmiin kirjautuville käyttäjille tulee määritellä ja rajata mahdollisimman suppeat, mutta kuitenkin tehtävien hoitamisen kannalta riittävät käyttöoikeudet. Henkilötietojen käsittelyä koskeva lainsäädäntö edellyttää, että rekisterinpitäjä on ennakkoon määritellyt sen, kenellä on oikeus tallentaa, poistaa tai muuttaa tietoja ja kenellä on oikeus hakea ja lukea niitä. Rekistereihin on myös tarvittaessa luotava järjestelmä, jonka avulla jokaisesta tehdystä toimenpiteestä, myös lukemisesta, jää merkintä tapahtumalokiin. (Pitkänen ym. 2013, 222–223.)

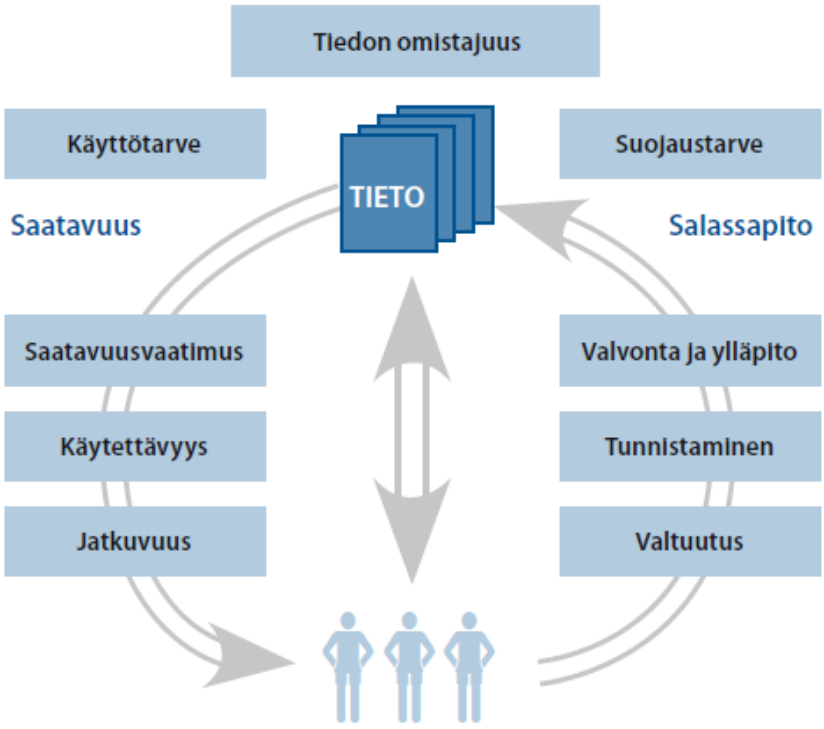
Kansallinen turvallisuusauditointikriteeristö KATAKRI on luotu työvälineeksi turvallisuustason tarkastajille yhteistyössä viranomaisten, elinkeinoelämän ja turvallisuusalan järjestöjen kanssa (Valtiovarainministeriö 2012, 28). Kriteeristön tarkoituksena on luoda yhtenäinen toimintamalli turvallisuustasojen auditointeihin. KATAKRI ja sen suositukset ovat myös suositeltava perustyökalu yrityksissä tapahtuvalle turvallisuustyölle. Yksi turvallisuusauditointikriteeristön päätavoitteista on auttaa yrityksiä omassa tietoturvan kehitystyössään. (Puolustusministeriö 2011, 3–4.) KATAKRIN materiaaliin kuuluu yli 160 kysymystä henkilöstö- ja tietoturvallisuuden sekä hallinnollisen ja fyysisen turvallisuuden alueilta eri vaatimustasoille ja sen materiaalia on vapaasti saatavissa Suomen Puolustusministeriön ylläpitämänä internetistä, osoitteesta http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf (Puolustusministeriö 2011, 1).

8.2 Hallinnollinen tietoturva

Hallinnolliseen tietoturvaan voidaan katsoa kuuluvan muun muassa riskien hallinta, henkilöstön koulutuksen ja ohjeistuksen, vastuiden ja tehtävien määrittelyt sekä riittävien tietoturvaresurssien ja taloudellisten edellytysten järjestämisen (Pitkänen ym. 2013, 215). Rekisterinpitäjä ei voi vahingon sattuessa vedota siihen, että tietojen riittävästä suojaamisesta aiheutuneet kustannukset olisivat olleet liian suuret. Tietoturva on otettava huomioon jo rekisterisuunnitelmaa laa-

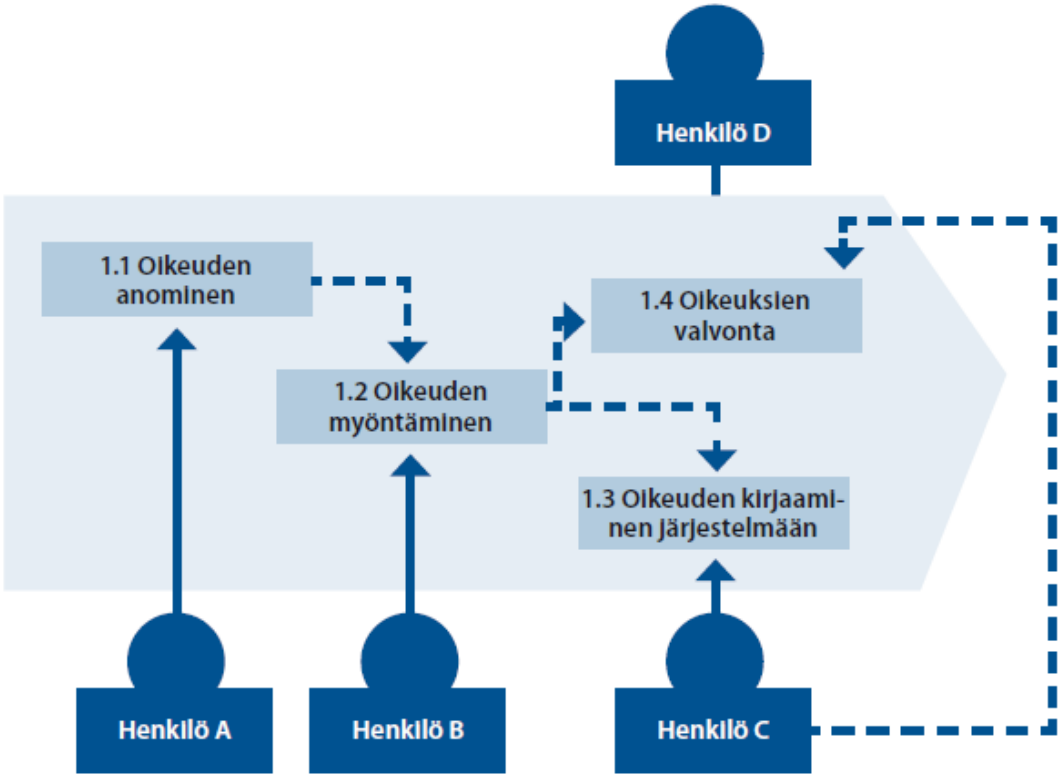
dittaessa ja samalla arvioitava se, onko rekisterinpitäjällä ylipäätään resursseja huolehtia henkilötietojen säilyttämisestä ja keräämisestä lain asettamien vaatimusten tasoisesti. Mikäli arviointi osoittaa, että riittävä tietoturvan taso tulisi käytettävissä oleviin resursseihin nähden liian kalliiksi, tulee rekisterin perustamishankkeesta luopua. (Pitkänen ym. 2013, 221.)

Olennaisena osana hallinnolliseen tietoturvaan kuuluvalla henkilöstöturvallisuudella tarkoitetaan tiedon käytettävyyteen ja salassapitoon liittyvien henkilöstöstä aiheutuvien riskien hallintaa. Henkilötietojen ja muun arkaluonteisen tiedon käsittely aiheuttaa aina suojaustarpeen ja toisaalta tiedon pitää olla sitä tarvitsevien henkilöiden käytettävissä. Saatavuuden ja suojauksen riippuvuussuhdetta ja haasteellisuutta on havainnollistettu kuviossa 8. Käytettävyyden kannalta tiedon tulee olla saatavilla ja käytettävissä yksinkertaisin keinoin. Suojausvelvollisuus taas edellyttää sitä, että tiedon käyttäjät on tunnistettu ja että heillä on valtuudet tietoa käyttää, mutta vain siinä määrin, kuin on välttämätöntä määriteltyjen tehtävien hoitamiseksi. Lisäksi tiedon käytön oikeellisuutta on valvottava asianmukaisesti. (Valtiovarainministeriö 2008, 12.)



Kuvio 8. Henkilöstöturvallisuus varmistaa tiedon saatavuuden ja salassapidon tasapainoa (Valtiovarainministeriö 2008, 12)

Henkilöstön toiminnasta tiedonkäsittelylle aiheutuvia riskejä voidaan vähentää hajauttamalla tehtäviä siten, että yksittäinen työntekijä ei saa olla vastuussa kuin yhdestä tietojenkäsittelyketjun osasta. Henkilöstöturvallisuudesta huolehtivassa organisaatiossa henkilö ei voi itse myöntää itselleen oikeuksia tietojärjestelmän käyttöön eikä kirjata tai valvoa omia järjestelmän käyttöön liittyviä tapahtumiaan. Toisaalta taas käyttöä valvovalla henkilöllä ei saa olla oikeuksia tietojärjestelmän operatiiviseen käyttöön tai oikeuksien myöntämiseen. Ketjussa on aina oltava erillinen oikeuksien myöntäjä, kirjaaja ja valvoja, kuten kuviossa 9 on esitetty. (Valtiovarainministeriö 2008, 30.)



Kuvio 9. Väärinkäytösten ehkäisy tehtäviä hajauttamalla (Valtiovarainministeriö 2008, 30)

8.3 Palvelun käyttäjän tunnistaminen ja todentaminen

8.3.1 Käyttäjätunnus ja salasana

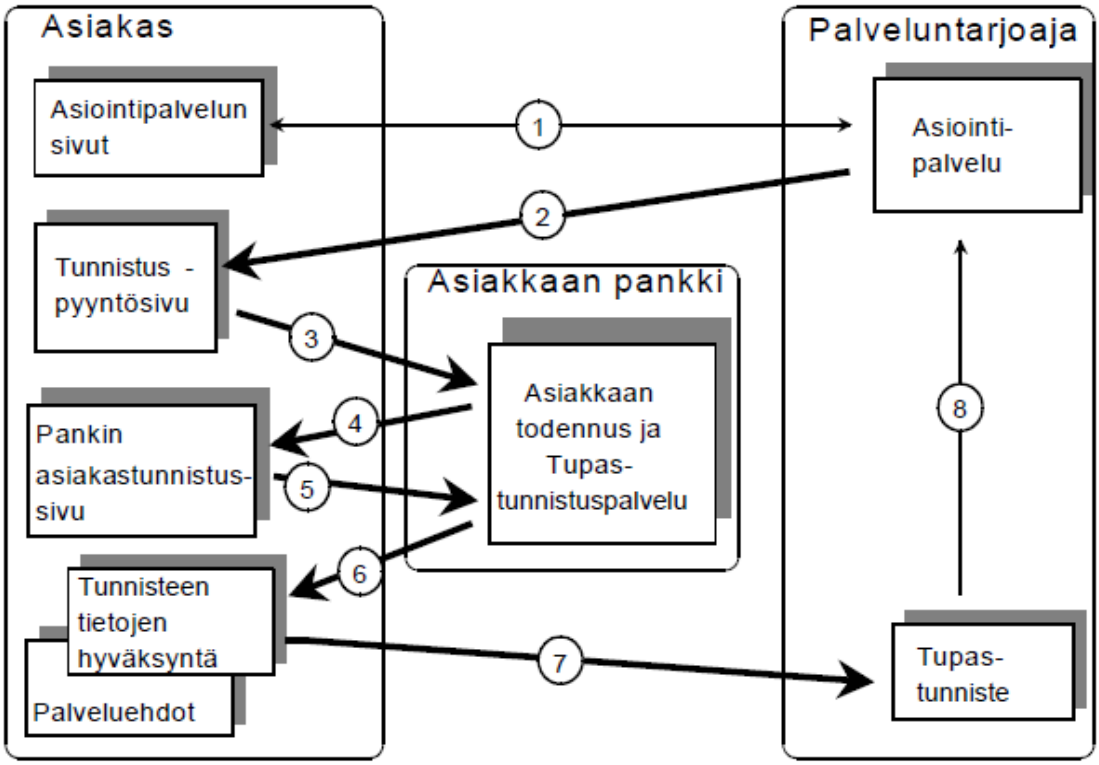
Yleisin tapa verkkopalvelussa tunnistautumiseen on käyttäjätunnuksen ja salasanan yhdistelmä. Asiakas itse luo ne rekisteröityessään palvelun käyttäjäksi tai esimerkiksi työnantajaorganisaation tietojärjestelmäylläpidosta vastaava tekee sen uuden työntekijän tullessa töihin. Käyttäjätunnus kertoo kuka palvelua käyttää ja salasana todentaa käyttäjän henkilöllisyyden (Järvinen 2003, 204). Tämä ei kuitenkaan ole kovin turvallinen menetelmä todentaa käyttäjän henkilöllisyys. Salasanat ja käyttäjätunnukset voivat paljastua tietomurron yhteydessä, tai käyttäjä on tallentanut tunnukset selaimen muistiin, jolloin kuka tahansa kyseisen koneen käyttäjä pääsee niihin käsiksi. Kaikki verkkopalvelut eivät myöskään käytä suojattua SSL -yhteyttä (Secure Sockets Layer) kirjautumisessa. Kun kirjautuminen tapahtuu suojaamattomalla yhteydellä, nettiliikennettä seuraava ulkopuolinen taho voi kaapata tiedot ja saada käyttäjätunnuksen ja salasanan haltuunsa. (Järvinen 2012, 121, 130.)

Käyttäjän itse luoma salasana ja käyttäjätunnus eivät täytä vahvan tunnistautumisen edellytyksiä. Vahvaa tunnistautumista vaaditaan esimerkiksi pankki- ja viranomaisasioinnissa. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista määrittelee vahvan sähköisen tunnistamisen niin, että henkilö yksilöidään ja tunnisteen aitous ja oikeellisuus todennetaan sähköistä menetelmää käyttäen niin, että vähintään kaksi seuraavista kolmesta vaihtoehdosta täyttyy:

- salasana tai jotain muuta sellaista, minkä käyttäjä tietää
- sirukortti tai jotain muuta sellaista, mitä tunnistusvälineen haltijalla on hallussaan
- sormenjälkeen tai johonkin muuhun tunnistusvälineen yksilöivään ominaisuuteen (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 1:2§).

8.3.2 Pankkitunnukset ja Tupas-tunnistuspalvelupalvelu

Tupas -lyhenne tulee sanoista ”Tunnistuspalvelu asiointipalvelujen tuottajille” ja palvelua ylläpitää Finanssialan Keskusliitto. Tupas -palvelun avulla yritys tai yhteisö, joka tarjoaa sähköisiä palveluita, voi tunnistaa asiakkaansa lähettämällä tunnistuspyynnön asiakkaalle (kuvio 10). Asiakas siirtyy oman pankkinsa tunnistuspalveluun ja kirjautuu sinne omilla verkkopankkitunnuksillaan. Tämän jälkeen Tupas -palvelu lähettää asiakkaalle kuittauksen tunnistautumisesta, jonka hyväksymisen jälkeen hän palaa palveluntarjoajan verkkosivulle ja tunnisteen tiedot välittyvät palveluntarjoajalle. Tupas -tunniste on ainutkertainen ja aikaleimalla sidottu sekä asiakkaaseen, että kyseiseen palvelutapahtumaan. (Finanssialan keskusliitto 2013a, 4.)



Kuvio 10. Tupas -tunnistuspalvelun kuvaus (Finanssialan keskusliitto 2013b, 16)

Pankkitunnukset koostuvat pankin antamasta käyttäjätunnuksesta ja vaihtuvista tunnusluvuista. Joillakin pankeilla kirjautuminen vaatii lisäksi salasanan. Tehdessään pankin kanssa sopimuksen verkkopalveluiden käytöstä, asiakas saa tunnuslukulistan, jonka luvut voivat olla kertakäyttöisiä tai satunnaisessa järjestyksessä toistuvia. Pankkitunnuksen myöntävä pankki tunnistaa pankkitunnuksen hakijan henkilökohtaisesti viranomaisen myöntämästä henkilöllisyyden luotettavasti todistavasta asiakirjasta ennen kuin ensimmäiset tunnukset luovutetaan asiakkaalle. (Finanssialan keskusliitto 2013a, 9.)

8.3.3 HST eli henkilön sähköinen tunnistaminen

Suomi oli ensimmäinen maa maailmassa, jossa kansalainen saattoi saada sähköisen henkilöllisyyden. Ensimmäinen HST -kortti myönnettiin pääministeri Paavo Lipposelle 1.12.1999. (Järvinen 2003, 190.)

Väestörekisterikeskus luo sähköisen henkilöllisyyden, jonka tunnuksena verkkoasioinnissa toimii sähköinen asiointitunnus (SATU). Asiointitunnus koostuu numeroista ja tarkistusmerkistä ja sen avulla yksilöidään Suomen kansalaiset ja väestötietojärjestelmään merkityt, Suomessa vakituisesti asuvat ulkomaalaiset. Tunnus aktivoidaan, kun kansalainen hankkii kansalaisvarmennetta hyödyntävän varmennekortin, esimerkiksi poliisin myöntämän sirullisen henkilökortin. (FINeID 2015.) SATU -tunnus on luotu jokaiselle henkilölle yhdessä henkilötunnuksen kanssa kesäkuusta 2003 alkaen. (Järvinen 2003, 193).

Kansalaisvarmenne perustuu julkisen avaimen menetelmään ja se sisältää muun muassa etu- ja sukunimen sekä sähköisen asiointitunnuksen. Kansalaisvarmenne toimii verkkoavaimena vahvaa tunnistautumista vaativissa sähköisissä palveluissa ja sähköisessä allekirjoituksessa. Kansalaisvarmennetta voi myös käyttää dokumenttien ja sähköpostien salaamisessa. (Väestörekisterikeskus, 2015.)

HST-kortin siru on mikropiiri, joka sisältää muistia ja prosessorin. Siruun on tallennettu kansalaisvarmenne, jonka perusteella käyttäjä tunnistetaan. Henkilö

todennetaan sirulla olevan avaimen perusteella. Avaimen käyttöä varten käyttäjän tulee antaa oikea PIN-koodi. Käyttäjä siis todentaa itsensä ensin kortille, joka sitten todentaa käyttäjän henkilöllisyyden verkkopalvelulle. (Järvinen 2003, 204.) Kortin käyttöä varten tarvitaan kaksi PIN-koodia, jotka sitovat kortin sen haltijaan (Järvinen 2003, 192). PIN1-koodia käytetään verkkopalveluihin kirjauduttaessa ja PIN2-koodia sähköisen allekirjoituksen luomiseen (FINeID, Kansalaisvarmenne, 2015). Toimiakseen HST-kortti vaatii lukulaitteen ja kortinlukijaohjelmiston (Järvinen 2003, 197).

Kansalaisvarmenteen sisältämän henkilökortin hakemus täytetään poliisin lupapalvelupisteessä tai poliisin sähköisessä asiointipalvelussa. Henkilökortin hakeminen vaatii kuitenkin aina käynnin poliisin lupapalvelupisteessä. Mukana tulee olla henkilöllisyystodistus, passi tai muu luotettava selvitys henkilöllisyydestä ja valokuva. Korttihakemus on jätettävä henkilökohtaisesti ja verkkopalveluun on kirjauduttava vahvaa tunnistautumista käyttäen. (Poliisi 2015.)

8.3.4 Mobiilivarmenne ja biometriset tunnisteet

Mobiilivarmenne on matkapuhelimen SIM-korttiin asennettu palvelu, joka toimii sähköisenä henkilötodistuksena. Palvelu on saatavissa DNA:n, Elisan ja Soneran liittymiin. (Tietosuojavaltuutetun toimisto, 2011.) Tunnistautuminen tapahtuu salatun tietoliikenneyhteyden kautta, eikä käyttäjän tunnuslukua lähetetä matkapuhelimesta minnekään, vaan se käsitellään ainoastaan SIM-kortilla (Mobiilivarmenne - Turvallisuus, 2015). Mobiilivarmenteen käyttö sisältää tyypillisesti kolme vaihetta. Palveluun kirjaudutaan omalla matkapuhelinnumerolla tai käyttäjätunnuksella. Tämän jälkeen matkapuhelimeen tulee tunnistuspyyntöviesti, joka kuitataan näppäilemällä oma tunnusluku. Puhelin lähettää tunnistustiedon palveluntarjoajalle ja palvelu on käytettävissä. (Mobiilivarmenne - Käyttö, 2015.)

Biometrisella tunnistuksella tarkoitetaan henkilön tunnistamista hyödyntäen sellaisia ihmiskehon ominaisuuksia, jotka lähes poikkeuksetta ovat jokaisella erilaiset. Tällaisia piirteitä ovat esimerkiksi sormenjäljet, silmän iiris, ääni ja kasvot. Biometristen tunnisteiden käytöllä on sekä etuja että haittoja. Biometrinen tun-

nistus voi nopeuttaa tunnistamista ja se koetaan usein perinteisiä tapoja helpommaksi keinoksi tunnistautua. Biometriset tunnisteet ovat aina mukana, eikä unohduksen vaaraa ole. Haittapuolena taas on se, että biometrisia tunnisteita voidaan kerätä ja väärinkäyttää siten, että henkilö ei itse huomaa tapahtunutta. Biometrinen tunnistaminen myöskään ei ole ehdottoman varma tapa tunnistaa henkilö, eikä sitä sen vuoksi tulisi käyttää tilanteissa, joissa vaaditaan vahvaa tunnistautumista, kuten esimerkiksi pankkiasioinnissa. (Tietosuojavaltuutetun toimisto, 2010, 2.) Biometrisiä tunnisteita kuten sormenjälkiä käytetään rikostekniseessä tutkinnassa ja muun muassa kulunvalvonnassa.

8.3.5 Henkilön fyysinen tunnistaminen

Lakitasolla ei suoranaisesti määrätä yleisistä henkilön fyysiseen tunnistamiseen käytettävistä asiakirjoista, mutta käytäntö on kuitenkin vakiintunut siten, että tietyt asiakirjat hyväksytään yleisesti tunnistamisasiakirjoiksi. Tällaisia vakiintuneessa käytössä olevia tunnistamisasiakirjoja ovat passin ja henkilökortin lisäksi ajokortti ja Kansaneläkelaitoksen myöntämä kuvallinen Kela-kortti. (Sisäasiainministeriö 2010, 30.)

Asetuksen tasolla säädetään, että virallisia poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja, jotka hyväksytään tunnistamisasiakirjoiksi passia ja henkilökorttia haettaessa, ovat passi ja henkilökortti (Valtioneuvoston asetus poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista 1 §). Poliisin myöntämien virallisten tunnistamisasiakirjojen luotettavuus perustuu sekä vaikeaan väärennettävyyteen että myöntämisprosessin luotettavuuteen. Sekä passia että henkilökorttia myönnettäessä poliisi tunnistaa asiakirjaa hakevan henkilön. Lisäksi nämä asiakirjat ovat vaikeasti väärennettäviä. (Sisäasiainministeriö 2010, 30–31.)

Ajokortti hyväksytään yleisesti tunnistamisasiakirjana esimerkiksi pankeissa, posteissa ja kaupoissa, vaikka se ei olekaan virallinen henkilöllisyyden todentava tunnistamisasiakirja (Sisäasiainministeriö 2010, 38). Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tosin säädetään, että

1.10.1990 jälkeen ETA-maassa myönnetty ja voimassa oleva ajokortti on hyväksyttävä tunnistamisasiakirja silloin, kun haetaan ensimmäisen kerran vahvan sähköisen tunnistamisen välinettä, esimerkiksi pankkitunnuksia (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009 3: 17 §).

Kaikkiin edellä kuvattuihin tunnistamismenetelmiin liittyy omat heikkoutensa, joiden vuoksi toisena henkilönä on mahdollista esiintyä. Kaikista suurimman tietoturvariskin muodostaa yleensä henkilö itse. Esimerkiksi vahvojen ja vaikeasti arvattavien salasanojen käyttämisen tärkeys saatetaan kyllä tiedostaa, mutta ne tallennetaan selaimen muistiin, juuri siksi, että ne ovat niin vaikeita muistaa. Etenkin aina mukana kannettavien mobiililaitteiden kohdalla tämä on suuri riski, koska näitä laitteita on helpompi varastaa kuin kotona olevaa tietokonetta.

Tunnistamisen ja käyttäjätietojen aitouden todentaminen on sikäli ongelmallinen ratkaista, että yleensä käytön helppous ja palvelun turvallisuus ovat kääntäen verrannollisia. Mitä helpompaa esimerkiksi internetpalveluun kirjautuminen on käyttäjälle, sitä helpompaa käyttäjätietojen selvittäminen on rikolliselle. Toisaalta taas suojattu ja suljettu ympäristö vaatii vaikeasti murrettavan salasanan ja kenties vielä mobiilivarmenteen käyttämisen. Palvelu on turvallinen, mutta asiakkaat voivat kokea sen käyttämisen hankalana, jolloin se jää käyttämättä.

9 POHDINTA

Tämän opinnäytetyön tavoitteena on ollut tutkia henkilötietojen keräämisen ja väärinkäytön muotoja. Tutkimuksen pääkysymyksenä on ollut selvittää, mitä identiteettivarkaus on ilmiönä, ja kuinka tavallinen ihminen voi itse ennaltaehkäistä identiteettivarkaan uhriksi joutumista. Tietoperustaan otimme mukaan myös henkilötietojen käsittelyä koskevaa lainsäädäntöä sekä tietoa erilaisista henkilörekistereistä. Identiteettitietojen lähteenä ovat usein julkiset rekisterit, sekä asiakkuuksiin liittyvät markkinointimateriaalit, joita haltuunsa hankkimalla saa yllättävän paljon tietoa toisesta ihmisestä.

Henkilötietojen väärinkäytöllä aiheutettujen vahinkojen skaala on laaja. Se voi olla internetissä tapahtuvaa kiusantekoa tai johtaa suuriin taloudellisiin tappioihin. Yksityisen ihmisen on hyvin vaikeaa korjata esimerkiksi maineen menetyksestä aiheutuvia vahinkoja, etenkin kun sosiaalisen median myötä miltei mikä tahansa tieto voi levitä muutamassa tunnissa ympäri maailman. Valheellisen tiedon leviämisen seurauksena saattaa olla esimerkiksi se, että henkilö ei saa työpaikkaa, koska hänestä löytyy epäilyttävää tietoa internetistä. Taloudellisten menetysten suhteen vahinkojen korjaaminen on yleensä hieman helpompaa, mutta ei yksinkertaista sekään. Identiteettivarkauden jälkiselvitykset voivat kaiken kaikkiaan olla vaikeita selvittää, eikä uhrille välttämättä ainakaan heti tule tietoon kaikki ne tilanteet, joissa hänen identiteettiään on käytetty luvatta. Siksi olisi hyvä olla olemassa jonkinlainen keskitetty ilmoitusjärjestelmä, johon väärinkäytöt voisi ilmoittaa sen sijaan, että joutuu ottamaan varalta yhteyttä moniin eri tahoihin.

Tehdessämme tätä opinnäytetyötä kiinnitimme huomiota muutamaan uutiseen, jotka liittyivät siihen, millaisen riskin uusi teknologia voi tuoda yksityisyydelle ja henkilötiedoille. Helsingin Sanomat uutisoi 9.2.2015, että elektroniikkavalmistaja Samsung on varoittanut ihmisiä välttämään arkaluonteisista asioista puhumista valmistamansa älytelevision lähellä. Laitteen kerrottiin tallentavan keskusteluita, jotta sen ääniohjaus toimisi ja se myös lähettää nauhoitteet kolmannelle osapuolelle. (Helsingin Sanomat 2015.)

Toinen vastaavan tyyppinen uutinen oli 16.3.2015 IT-viikko verkkojulkaisussa. USA:ssa nousi kohu leluvalmistaja Mattelin suunnitelmista tuoda markkinoille Barbie-nukke, joka kuuntelee sillä leikkivän lapsen puhetta ja myös vastaa lapselle. Toimintaperiaatteena on, että nukke lähettää puheen Mattelin palvelimelle, jossa puhe analysoidaan ja siihen luodaan vastaus, jonka nukke kertoo lapselle. (It-viikko 2015.) Muun muassa nämä uutiset saivat meidät pohtimaan, millaisia yhä kasvavia riskejä liittyy siihen, että meistä kerätään yhä enemmän ja yksityisempää tietoa rekistereihin ja tietovarastoihin, joista emme itse välttämättä tiedä mitään. Edellä mainitusta Barbie-nukesta kertova uutinen sai meidät myös pohtimaan tuotekehityksen jatkoa. Nopeasti kehittyvän teknologian avulla voisi kuvitella olevan hyvinkin lähellä aika, että kyseisen nuken sinisilmät toimivat kamerana ja tallentavat kuvaa mahdollista myöhempää käyttöä varten. Epäilemättä pienet tytöt rakastaisivat vuorovaikuttavaa Barbie-nukkea, mutta miten vanhemmat voivat olla varmoja siitä, että nukke pysyy puheissaan lapsen tasolla eikä esimerkiksi ryhdy muokkaamaan lapsen mielipiteitä tai manipuloi häntä muuten.

Esineiden internet tulee olemaan myös suuri haaste tietosuojalle. Amerikkalainen tietoturvayhtiö Veracoden tuoreen raportin mukaan monet kuluttajille suunnatut kodin laitteet ovat ilman vahvoja tietoturvatoimintoja. Tutkimuksessa testatuista kuudesta laitteesta viidessä todettiin haavoittuvuuksia tietoturvan suhteen. Laitteiden suunnittelussa tietoturva ja yksityisyys eivät useinkaan ole tärkeimmät lähtökohdat, joten laitteet voivat lisätä riskiä esimerkiksi asuntomurroille. (Veracode). Tietosuoja ja tietoturva ovat kuitenkin niin tärkeitä asioita, että niiden toimivuuteen tulee panostaa. Tietosuoja kaikissa kuluttajalaitteissa tulee olla riittävän hyvin toteutettu valmistajan toimesta, sillä kaikki ihmiset eivät voi olla tekniikan asiantuntijoita.

Esineiden internetin yleistyessä myös erilaisten käyttäjiä profiloivien toimijoiden voi olettaa lisääntyvän. Profiloinnin tarkoituksena on auttaa yrityksiä kohdentamaan markkinointia, joten toiminnassa liikkuu valtavasti rahaa. Käyttäjistä kerättävä tiedon määrä on koko ajan kasvamassa ja toisaalta kerätyn tiedon hyödyntäminen tulee yrityksille koko ajan edullisemmaksi ja tekniikaltaan kehittyneem-

mäksi. Lainsäädäntö ei ole pysynyt kehityksessä mukana ja näkisimmekin, että asialle pitäisi nopeasti tehdä jotain.

Nykyinen henkilötietolaki on Suomessa tullut voimaan vuonna 1999 ja sen voi katsoa olevan ajastaan jäljessä joiltain osin. Esimerkiksi vielä vuonna 2003 Euroopan yhteisöjen tuomioistuin EYT katsoi, että yksityisen henkilön työtovereistaan keräämät ja internetissä julkaistut henkilötiedot, kuten nimi, ammatti ja kuva, olivat henkilötietodirektiivin tarkoittamaa osittain tai kokonaan automatisoitua henkilötietojen käsittelyä ja siten henkilörekisterejä koskevan lainsäädännön piirissä. Sosiaalisen median yleistyttyä on vaikea nähdä millä tavalla esimerkiksi normaali Facebook-sivu, jolla näkyvät ystävien henkilötiedot ja kuvat, poikkeaisi esimerkin kaltaisesta aiemmin kielletystä internetsivusta. (Pitkänen ym. 2013, 31–32.)

Euroopan unionin yleistä tietosuoja-asetusta on valmisteltu useita vuosia. Komissio on vuonna 2010 nostanut esille kasvavan tarpeen ajantasaistaa yksityisyyden suojaa koskevaa lainsäädäntöä Euroopan unionin alueella ja samalla huomioida se, että eurooppalaisista kerättyä tietoa käsitellään yhä enemmän myös unionin ulkopuolella. Ehdotus yleiseksi tietosuoja-asetukseksi on komission toimesta annettu vuonna 2012, mutta asian käsittely on edelleen kesken. (Oikeusministeriö 2015.)

Tiedon käsittelyä ja tietosuojaan liittyviä seikkoja selvittäessämme pohdimme tiedon luokittelun tärkeyttä. Kaikkea tietoa ei ole tarpeen säilyttää ja vain vähäinen tietomäärä koko valtavasta massasta on sellaista, että se täytyy tallentaa pitkiksi ajoiksi. Olisi hyvä, että sähköiselle tiedolle voisi määritellä arkistointiajan, jonka jälkeen sekä alkuperäinen dokumentti että sen kopiot tuhoutuisivat automaattisesti. Tieto olisi siis ns. aikahajoavaa, jolloin sellaista tietoa, jota kukaan ei koskaan tarvitse, ei turhaan säilytetä. Etenkin arkaluonteisen tiedon säilytyksessä on tietosuojan kannalta merkittävä huomata myös se, että pelkkä tiedoston poistaminen (deletointi) ei tarkoita sitä, että se olisi hävitetty lopullisesti, edes silloin, kun roskakori on tyhjennetty. Poistettuja tietoja on nimittäin mahdollista palauttaa. Tiedon lopullisen tuhoamisen voi tehdä erilaisilla ohjelmilla, jotka

hävittävät tiedon ylikirjoittamalla tai niin, että kiintolevy magnetoidaan. Tietysti tallennusväline voidaan hajottaa mekaanisesti niin, että siitä tulee lukukelvoton, jolloin kukaan ei enää pääse tietoon käsiksi. (Yhteiskuntatieteellinen arkisto 2015).

Tämän opinnäytetyön tekemisen suurimpia haasteita on ollut tiedon löytäminen. Aihe on Suomessa vielä sen verran vähän tutkittu, että mitään kovin kattavia lähdeteoksia ei vielä ole tehty. Jouduimmekin koostamaan aineiston todella monesta lähteestä. Ulkomaisia lähteitä hyödynsimme jonkin verran, mutta meillä ei ollut tämän työn puitteissa mahdollista perehtyä englanninkieliseen tietotekniseen ja juridiseen erityissanastoon niin tarkoin, että olisimme voineet perehtyä niihin enempää kuin nyt olemme tehneet.

Rajasimme työmme koskevaan vain Suomea lähinnä sen ajankohtaisuuden vuoksi, mutta myös siksi, että pystyisimme käsittelemään asiat hieman syvällisemmin. Tutkinnan laajetessa maantieteellisesti kovin laajaksi, työ jää muilta osin helposti pintapuoliseksi. Identiteettivarkauksien laatua ja määrää sekä niiden rangaistavuutta eri puolella maailmaa olisi kuitenkin haastavaa ja mielenkiintoista tutkia. Yksi seikka, mikä puoltaa jatkotutkimusta on se, että suuri joukko suomalaisia ihmisiä työskentelee ulkomailla, opiskelee vaihto-oppilaina, tekee työharjoittelua tai muuten vain lomailee maissa, joissa identiteettivarkauksien määrä on paljon suurempi kuin Suomessa. Ehkä tietoisuus riskeistä lisäisi huolellisuutta omien henkilötietojen käsittelyssä. Toisaalta myös jatkotutkimus identiteettivarkauksien laadusta ja määrästä Suomessa sen jälkeen, kun se on rikoslaissa säädetty, olisi mielenkiintoinen toteuttaa.

Vaikka tässä työssä on esitelty monia uhkia ja riskejä, mitä sekä fyysisessä että varsinkin sähköisessä maailmassa piilee, ei niistä kannata tehdä mörköä itselleen. Terveellä maalaisjärjen käytöllä ja maltilla väistää jo monta mahdollisesti kohtaavaa uhkaa. Ylen aamu-tv:n haastattelema tietosuojavaltuutettu Reijo Aarnio sanoi osuvasti, että identiteettivarkauden kohde ei ole ikäkysymys. Riskiryhmään kuuluvat hänen mielestään ne, jotka eivät pidä silmiään auki. (Yle, 17.2.2014). Tietosuojan merkitys on kuitenkin tärkeä ymmärtää, ja sen vuoksi

se tulisi olla yhtenä osana lasten ja nuorten koulutuksessa ja kasvatuksessa, josta vastuussa ovat sekä koulu että vanhemmat.

LÄHTEET

Aalto, T – Uusitalo, M. 2009. Nettielämää. Sosiaalisen median maailmat. Jyväskylä: Gummerus kirjapaino.

Aktia 2015. Kotivakuutus, vakuutusehdot 88K a, voimassa 1.1.2015 alkaen. Viitattu 4.3.2015. Osoitteessa: http://www.aktia.fi/documents/10552/53172/Aktia+Kotivakuutusehdot+88K+a.pdf/9eecb34f-6e29-4fc5-a3bf-edd8fc9f24ff.

Aktia Pankki 2014. Tutkimus: Henkilötietoja varjellaan huonosti. Viitattu 3.3.2015. Osoitteessa: http://investors.aktia.fi/m/index.php?p=press&s=detail&afw_id=1316812&afw_lang=fi.

Andreasson, A. – Koivisto J. 2013. Tietoturvaa toteuttamassa. Tallinna: AS Pakett.

Biegelman, M. 2009. Identity Theft Handbook: Detection, Prevention and Security. John Wiley & Sons. Viitattu 15.3.2015-16.3.2015. Osoitteessa: http://ez.lapinamk.fi:2054/lib/ramklibrary/reader.action?docID=10297848&ppg=29.

Council of Europe Recommendation CM/Rec (2010) 13. Viitattu 22.3.2015. Osoitteessa: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

ETLA 2015. Suomalainen teollinen internet – haasteesta mahdollisuudeksi. ETLA raportti nro 42/5.1.2015. Viitattu 6.4.2015. Osoitteessa: http://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-42.pdf.

Euroopan unionin perusoikeuskirja 200/C 364/01. Viitattu 19.3.2015. Osoitteessa: http://www.europarl.europa.eu/charter/pdf/text_fi.pdf.

FiCom 2011. Tietoturvaviikko 2011. Oma identiteetti kullan kallis. Viitattu 17.3.2015. Osoitteessa: http://www.ficom.fi/ajankohtaista/ajankohtaista_1_1.html?Id=1297062240.html.

Finanssialan keskusliitto 2013a. Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet V2.0c 2.12.2013. Viitattu 20.3.2015. Osoitteessa: http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas_tunnistusperiaatteet_v20c_FI.pdf

FINE. Vakuutus- ja rahoitusneuvonta. Viitattu 19.3.2015. Osoitteessa: https://www.fine.fi/finanssitietoa/pankkiasiat/turvallisuus-ja-tietosuoja.html.

FINeID 2015. Sähköinen henkilöllisyys ja varmenteet. Viitattu 2.2015. Osoitteessa: http://www.vrk.fi/default.aspx?id=134.

Forss, M. 2014. Fobban sosiaalisen median selviytymisopas. Helsinki: Crime time.

Heinonen, R. 2001. Digitaalinen minä. Helsinki: Edita Oyj.

Heinonen, R. 2006. Luottamus verkkoasiointiin edellyttää yksityisyyden suojaa. Luoti-artikkeli 3/2006. Viitattu 23.2.2015. Osoitteessa: http://www.lvm.fi/fileserver/3_2006.pdf.

Helsingin Sanomat 2015. Yhdysvalloissa jättimäinen tietomurto 5.2.2015. Viitattu 23.2.2015. Osoitteessa: http://www.hs.fi/ulkomaat/a1423104868529.

Helsingin Sanomat 2015. Älytelevisio voi kuunnella ja välittää keskustelusi. Viitattu 6.4.2015. Osoitteessa: http://www.hs.fi/tekniikka/a1423456969588

Henkilötietolaki 22.4.1999/523.

Heuer, S. & Tranberg, P. 2013. Älä kerro kaikkea! Itsepuolustusopas verkkoon. Helsinki: Talentum

Hovi, A. – Hervonen, H. – Koistinen, H. 2009. Tietovarastot ja business intelligence. Jyväskylä: WSOYpro/Docendo-tuotteet.

It-viikko 2015. Barbie salakuuntelee: Peruste estää myynti kokonaan? Viitattu 16.3.2015 ja 6.4.2015. Osoitteessa: http://www.itviikko.fi/uutiset/2015/03/16/barbi-salakuuntelee-peruste-estaa-myynti-kokonaan/20153323/7.

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo Finland Oy.

Järvinen, P. 2010. Yksityisyys Turvaa digitaalinen kotirauhasi. Jyväskylä: Docendo Finland Oy.

Järvinen, P. 2012. Arjen tietoturva vinkit ja ratkaisut. Jyväskylä: Docendo Finland Oy.

Kalliopuska, M. 2005.Psykologian sanasto. Keuruu: Otavan Kirjapaino Oy.

Kangasniemi, T 2012. Identiteettivarkaudet - haasteita rikostutkinnalle ja -oikeudelle, paljon vaivaa ja harmia uhrille. Julkaisussa Perus- ja ihmisoikeudet rikosprosessissa / toim. Laura Ervo, Raimo Lahti, Jukka Siro. - Helsinki : Helsingin hovioikeus. Viitattu 8.2.2015, 8.3.2015. Osoitteessa: http://www.oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/perus-jaihmisoikeudetrikosprosessissa2012/MIpzV15CB/10_Identiteettivarkaudet_-_haasteita_rikostutkinnalle_ja_-oik..._Tea_Kangasniemi.pdf.

Kansalaisyhteiskunta 30.9.2011. Facebook-kielen lyhyt oppimäärä, osa 1. Viitattu 15.3.2015. Osoitteessa: http://www.kansalaisyhteiskunta.fi/markkinointi/blogitekstit_aihepiireittain/palvelut/facebook-kielen_lyhyt_oppimaara_osa_1.895.blog.

Kansaneläkelaitos 2011. Kelan atk-rekisterit ja niiden sisältämät tiedot rekistereittäin. 15.11.2011. Viitattu 19.3.2015. Osoitteessa: http://uudistuva.kela.fi/in/internet/liite.nsf/net/310806125816mk/$file/atk.pdf.

Kansaneläkelaitos 2015. Asiakastietojen rekisterit. 2.3.2015. Viitattu 30.3.2015. Osoitteessa: http://www.kela.fi/tietosuoja.

Kirjallinen kysymys KK 739/2010 vp. Viitattu 18.2.2015. Osoitteessa: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/kk_739_2010_p.shtml.

Kirjallinen kysymys KK 855/2012 vp. Viitattu 18.2.2015. Osoitteessa: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/kk_855_2012_p.shtml.

Korttiturvallisuus. 26.9.2014.: KRP: Korttikopiointi on pysynyt marginaali-ilmiönä. Viitattu 16.3.2015. Osoitteessa: https://www.korttiturvallisuus.fi/Uutisia/2014/Vantaan-Sanomat-KRP-Korttikopiointi-on-pysynyt-marginaali-ilmiona/.

Kotilainen, S 2013. Miljardit laitteet liitetään nettiin. MbNet 12.11.2013.Viitattu 29.3.2015.

Lagus, A. 2015. Esineiden internet on jo totta teollisuudessa. Tietosuoja 1/2015.

Laki ajoneuvoliikennerekisteristä 13.6.2003/541

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 21.8.2009/661

Lakivaliokunnan mietintö 15/2005 vp. Viitattu 19.3.2015. Osoitteessa: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/lavm_15_2005_p.shtml. 19.3.2015..

Liikenne- ja viestintäministeriö. 2013. Oikeudenmukaista ja älykästä liikennettä. Tietoturva ja yksityisyyden suoja - alatyöryhmä. Viitattu 23.2.2015. Osoitteessa: https://www.lvm.fi/docs/fi/2497123_DLFE-22568.pdf.

Limnell, J & Majewski, K – Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Linden, M 2012. Identiteetin- ja pääsynhallinta. Viitattu 23.3.2015. Osoitteessa: http://www.cs.tut.fi/~linden/iam-pruju.pdf.

Mobiilivarmenne - Käyttö 2015. Viitattu 11.3.2015. Osoitteessa: http://www.mobiilivarmenne.fi/fi/use.

Mobiilivarmenne - Turvallisuus 2015. Viitattu 11.3.2015. Osoitteessa: http://www.mobiilivarmenne.fi/fi/security.

Moilanen, K. 2015. Valmistaja varoittaa: Älyteleviso voi kuunnella ja välittää keskustelusi. Helsingin Sanomat 9.2.2015.

MTV Uutiset 2015. Epäily: Sairausvakuutusyhtiön jättimurron takana Kiinan tukemat krakkerit? 6.2.2015. Viitattu 28.2.2015. Osoitteessa: http://www.mtv.fi/uutiset/it/artikkeli/epaily-sairasvakuutusyhtion-jattimurron-takana-kiinan-tukemat-krakkerit/4760652.

MTV Uutiset 2015. Myyjällä supermuisti - painoi asiakkaiden luottokorttitiedot hetkessä muistiin 24.3.2015. Viitattu 26.3.2015. Osoitteessa: http://www.mtv.fi/uutiset/rikos/artikkeli/myyjalla-supermuisti-painoi-asiakkaidenluottokorttien-tiedot-hetkessa-muistiin/4932528.

mySafety Oy. 2015. ID-turva – suojaa ja vakuuta henkilötietojasi 24/7. Viitattu 4.3.2015. Osoitteessa: https://www.mysafety.fi/palvelut/id-turva.

Nixu Oyj. Sisälle PCI-terminologian saloihin. 6.11.2009. Viitattu 16.3.2015. Osoitteessa: http://www.nixu.com/fi/blogi/2009-11/sis%C3%A4lle-pci-terminologian-saloihin-%E2%80%93-mit%C3%A4-onkaan-skimmaus.

Oikeusministeriö 2013. Identiteettivarkaus Lausuntotiivistelmä Mietintöjä ja lausuntoja 47/2013. Viitattu 8.2.2015. Osoitteessa: http://oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1380522953940/Files/OMML_47_2013_Idetiteetti_laustiiv_34s.pdf.

Oikeusministeriö 2015. Euroopan unionin tietosuojalainsäädännön uudistaminen. Viitattu 22.3.2015. Osoitteessa: http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html.

Oikeuspoliittinen tutkimuslaitos 2013. Suomalaiset väkivallan ja omaisuusrikosten kohteena 2012. Kansallisen rikosuhritutkimuksen tuloksia. Verkkokatsauksia 28/2013. Viitattu 21.2.2015. Osoitteessa: http://www.optula.om.fi/material/attachments/optula/julkaisut/verkkokatsauksia-sarja/5UFBrKW1f/verkko_28.pdf.

OLAF Euroopan petostentorjuntavirasto 2013. Yhteenveto OLAF:in toiminnasta vuonna 2011 ja esimerkkitapauksia 1.tammikuuta – 31. joulukuuta 2011. Viitattu 28.2.2015. Osoitteessa: http://ec.europa.eu/anti_fraud/documents/reports-olaf/2011/ar_summary_fi.pdf.

Peltier, T. Information systems security. Social Engineering: Concepts and solutions. Viitattu 22.3.2015. Osoitteessa:

http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm#.VQ6Hr_msVHV.

Peltokorpi, J. & Norppa, K. 2015. Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Viro: Print Best.

Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Helsinki: Talentum Media Oy.

Poliisi 2015. Henkilökortin hakeminen. Viitattu 11.3.2015.Osoitteessa: http://poliisi.fi/henkilokortti/henkilokortin_hakeminen.

Puolustusministeriö 2011. KATAKRI Kansallinen turvallisuusauditointikriteeristö versio II 2011. Viitattu 22.3.2015. Osoitteessa: http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf.

Rikoslaki 19.12.1889/39.

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Viro: Print Best.

Salminen J. 2010. Identiteettivarkaus: Rikolliset jopa liimaavat roskikseen revittyjä papereita. Suomen kuvalehti. 4.3.2010. Viitattu 16.2.2015. Osoitteessa: http://suomenkuvalehti.fi/jutut/kotimaa/talous/identiteettivarkaus-rikolliset-jopa-liimaavat-roskikseen-revittyja-papereita/.

Salo, I. 2013. Big data, tiedon vallankumous. Jyväskylä: Docendo Oy.

Salo, I. 2014. Big data & pilvipalvelut. Jyväskylä: Docendo Oy.

Sanastokeskus TSK ry. 2003. Tietotekniikan termitalkoot. Viitattu 17.3.2015. Osoitteessa: http://www.tsk.fi/tsk/termitalkoot/en/node/267?page=get_id&id=ID0214&vocabulary_code=TSKTT.

Sanastokeskus TSK ry. 2004. Tiivis tietoturvasanasto. Viitattu 28.2.2015. Osoitteessa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf.

Sisäasiainministeriö 2010. Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäinen turvallisuus. Sisäasiainministeriön julkaisuja 32/2010. Viitattu 8.2.2015. Osoitteessa: http://www.intermin.fi/julkaisu/322010?docID=24918.

S-kanava 2014. Asiakasomistaja- ja asiakasrekisteri. Viitattu 19.3.2015. Osoitteessa: https://www.s-kanava.fi/web/s/s-kanavan-rekisteriseloste.

Suomen Asiakastieto Oy. 2015. Oma luottokielto. Viitattu 4.3.2015. Osoitteessa: https://www.omatieto.fi/luottotiedot/actValitseOlk.do

Suomen Asiakastieto Oy. 2015. Omatieto-palvelu. Viitattu 4.3.2015. Osoitteessa: https://www.omatieto.fi/luottotiedot/Aloitus.jpf?raportti=8.

Suomen Asiakastieto Oy. 2015. Tietoa luottotiedoista. Viitattu 4.3.2015. Osoitteessa: https://www.omatieto.fi/Omatieto-ukk_1.htm.

Suomen perustuslaki 11.6.1999/731.

suomi.fi 2015. Henkilötiedot ja nimet. Viitattu 8.2.2015. Osoitteessa: http://www.suomi.fi/suomifi/suomi/palvelut_aiheittain/laki_ja_oikeusturva/tietosuoja_ja_henkilotiedot/henkilotiedot_ja_nimet/index.html.

Tor Project 2015. Viitattu 6.4.2015. Osoitteessa: https://www.torproject.org/.

Viestintävirasto 2015. Metadata kertoo enemmän kuin luulit. Tietosuoja 1/2015.

Tietosuoja 2011. Älykäs koti on verkossa. Viitattu 6.4.2015. Osoitteessa: https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=2777.

Tietosuojavaltuutetun toimisto 2010a. Biometrinen tunnistus, mikä se on? 27.7.2010. Viitattu 18.3.2015. Osoitteessa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf.

Tietosuojavaltuutetun toimisto 2014. Euroopan neuvoston antamia suosituksia. 17.2.2014. Viitattu 22.3.2015. Osoitteessa: http://www.tietosuoja.fi/fi/index/lait/kansainvalisetnormitjaohjeet/euroopanneuvostonantamiasuosituksia.html.

Tietosuojavaltuutetun toimisto 2010b. Henkilötietolain seuraamusjärjestelmä 27.7.2010. Viitattu 19.3.2015. Osoitteessa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltutetuntoimisto/oppaat/6JfprbX39/Henkilotietolain_seuraamusjarjestelma.pdf.

Tietosuojavaltuutetun toimisto 2
010c. Identiteettivarkaus, mikä se on? 27.7.2010. Viitattu 8.3.2015. Osoitteessa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltutetuntoimisto/oppaat/6Jfpv4mWV/Identiteettivarkaus_mika_se_on.pdf.

Tietosuojavaltuutetun toimisto 2010d. Henkilötietolain mukainen ilmoitusvelvollisuus. 27.7.2010. Viitattu 22.3.2015. Osoitteessa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltutetuntoimisto/oppaat/6Jfpr4Tsl/Henkilotietolain_mukainen_ilmoitusvelvollisuus.pdf

Tietosuojavaltuutetun toimisto 2011. Mobiilivarmenne uusi vaihtoehto vahvaan sähköiseen tunnistamiseen. 27.6.2011. Viitattu 18.3.2015. Osoitteessa: http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2011/06/mobiilivarmenneuusivaihtoehtovahvaansahkoiseentunnistamiseen.html.

Valtioneuvoston asetus poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista 707/2006.

Valtioneuvosto 2013. Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 7.3.2013. Viitattu 19.3.2015. Osoitteessa: http://oikeusministerio.fi/material/attachments/om/valmisteilla/lakihankkeet/seuraamusjarjestelma/6G8gRl1Wx/JR-strategia_PTJ_SUOMI.pdf.

Valtioneuvosto 2009. Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta. 5.3.2009. Viitattu 19.3.2015. Osoitteessa: http://www.lvm.fi/docs/fi/463318_DLFE-6745.pdf.

Valtiovarainministeriö 2008. Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietotuvallisuutta. VAHTI 2/2008. Viitattu 2.4.2015. Osoitteessa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229.

Valtiovarainministeriö 2010. Sosiaalisen median tietoturvaohje Vahti 4/2010. Viitattu 15.3.2015. Osoitteessa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10128&groupId=10229. Viitattu 15.3.2015.

Valtiovarainministeriö 2013. Toimitilojen tietoturvaohje Vahti 2/2013. Viitattu 23.3.2015. Osoitteessa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10128&groupId=10229.

Valtiovarainministeriö 2013. Teknisen ICT-ympäristön tietoturvataso-ohje Vahti 3/2012. Viitattu 22.3.2015. Osoitteessa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10128&groupId=10229.

Vanto, J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro Oy.

Veracode. The Internet of Things Poses Cyberscurity Risk. Viitattu 8.4.2015. Osoitteessa: https://info.veracode.com/whitepaper-the-internet-of-things-poses-cybersecurity-risk.html.

Verkkouutiset. 8.2.2015. SS:Silppua henkilötiedot – Identiteettivarkaus voi olla pitkäaikainen harmi. Viitattu 7.3.2015. Osoitteessa: http://www.verkkouutiset.fi/kotimaa/identiteettivarkaus_harmi_vahinko-31725.

Verohallinto 2015. Verohallinnon rekisterit. Viitattu 18.3.2015. Osoitteessa: http://vero.fi/fi-FI/Tietoa_Verohallinnosta/Julkisuus_ja_tietosuoja/Verohallinnon_rekisterit.

Viestintävirasto 2014. Näin meitä huijataan. Ohje 1/2014. Viitattu 28.2.2015. Osoitteessa:

https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Nain_meita_huijataan.pdf.

Viestintävirasto 2015. Metadata kertoo enemmän kuin luulit. Tietosuoja 1/2015 Viitattu 28.3.2015.

VTT Tietotekniikka 2000. Tutkimusraportti TTE1-2000-32. 24.11.2000. Tiedon louhinta ja asiakkuudenhallinta –tuoteselvitys. Viitattu 22.3.2015. Osoitteessa: http://virtual.vtt.fi/virtual/datamining/publications/datamining_crm_tuoteselvitys.html#1.

Väestörekisterikeskus 2013. Viitattu 8.2.2015 - 30.3.2015. Osoitteessa: http://www.vrk.fi.

Väestörekisterikeskus 2013. Kiinteistötiedot. Viitattu 29.3.2015. Osoitteessa: http://www.vrk.fi/default.aspx?id=170.

Väestötietojärjestelmä 2013. Henkilötunnus. Viitattu 30.3.2015. Osoitteessa: http://www.vrk.fi/default.aspx?id=167.

Yhteiskuntatieteellinen arkisto 16.3.2015. Aineistonhallinnan käsikirja. Fyysinen säilytys. Viitattu 8.4.2015. Osoitteessa: http://www.fsd.uta.fi/tiedonhallinta/osa9.html.

Yle TV2. Poliisitv. Taantuma houkuttaa talousrikoksiin. Viitattu 23.3.2015. Osoitteessa: http://yle.fi/vintti/ohjelmat.yle.fi/poliisitv/raportit/taantuma_houkuttaa_talousrikoksiin.html.

Yle uutiset. 17.10.2014. Viitattu 16.2.2015. Osoitteessa: http://yle.fi/uutiset/identiteettivarkaus_ei_vaadi_kuin_yhden_puhelinsoiton__laki_laahaa_kilometrin_jaljessa/7530559.

Yle uutiset. 25.7.2014. Viitattu 23.2.2015. Osoitteessa: http://yle.fi/uutiset/tallaisia_ovat_suomalaisiin_kohdistuvat_identiteettivarkaudet__harvemmin_nama_selviavat/7303477.

Yle. Mitä jos identiteettisi viedään? 17.2.2014. Viitattu 21.2.2015. Osoitteessa: http://areena.yle.fi/tv/2659891.

Kuva 1. Tarkistusmerkin laskeminen. Väestörekisterikeskus 2013. Viitattu 30.3.2015. Osoitteessa: http://www.vrk.fi/default.aspx?id=167.

Kuva 2. Henkilötietojen käsittelyn elinkaarimalli. Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Helsinki: Talentum Media Oy.

Kuva 3. Muutama minuutti surffailua yleisesti käytetyillä sivuilla. Kuvakaappaus Lightbeam-ohjelmasta.